RiskCAT 61508 V6.1
User’s Manual

20. February 2010

RiskCAT 61508

Requirements on
High Quality Embedded Systems and
their Software

A Tool of the

***C**ode **A**nalyzer **T**ool **S**et*

User's Manual

CATS Software Tools GmbH, Hamburg
www.cats-tools.de

Contents

Figures

Version Index

Date of User's Manual	For RiskCAT Version	Changes	Author
2002-10-26			G. Glöe
2004-06-05 2004-07-21		• aus Abschnitt 2.1 das De-Installieren der Demo-Version rausgenommen • Key-Word „IF NOT" aufgenommen • Die Erweiterungen für V5 aufgenommen	G. Glöe
2004-08-11		• midas.dll entfernt • Installation, De-Installation überarbeitet • Anhang 7.2, Dokumente, überarbeitet	G. Glöe
2004-10-22		• zusätzliche Dokumente und Aktivitäten korrigiert • im Abschnitt 1 gleich zu Beginn neben dem Bild: Software -> embedded system • Zusammenhang der Bildschirmteile eingefügt • keine Anwahl als Precondition für gute Selectionen eingefügt • Grössenänderung Normenfenster beschrieben	G. Glöe
2005-12-17	V5.4	• in 1. die farbliche Unterscheidung der V4 Funktionalität rausgenommen • in 4.7 und 4.8 ergänzt "Appendix ... of this manual." • 7.3 gelöscht • Screen Shots zum Teil ausgewechselt wegen Änderungen am pdf viewer • Screen Shots / Erläuterung neu wegen neuer Bezeichnung der areas • Änderungen von Chris Hills eingearbeitet • Von Lieferung über CD auf USB memory stick umgestellt • Den Anfang von Kapitel 6.4 (Text vor 6.4.1) überarbeitet	G. Glöe
2006-02-12	V5.5	• Doors Export ergänzt • Caliber RM Export ergänzt	G. Glöe
2006-08-28	V5.6	• Structure of the functions adopted to the RiskCAT poster	G. Glöe

2008-08-12	V5.8	- In Kap 10.1 die Quelle für shall, should geändert von IEC 61226, Kap 3, nach Introduction (Grund ist zweite IEC 61226 Fassung, 2005-02) - Two misprints corrected in chapter "About part 1 of the standard". - Three misprints corrected in chapter "About part 2 of the standard". - Chapter added „Abbreviations used in this Manual" - Screenshots revised	G. Glöe
2008-12-06	V5.9	- Screenshots aktualisiert - Kapitel 4 (erforderlicher SIL) vollständig überarbeitet - Measure -> Prescription	G. Glöe
2010-01-20	V6.1	New document basis derived from an intermediate version of the RiskCAT 26262 V6.1 User's Manual from 2010-02-01	G. Glöe

Acknowledgements and trademarks

All trademarks used in this manual are acknowledged.

ARTiSAN Studio is a trademark of ARTiSAN Software Tools Ltd.

CaliberRM is a trademark of Borland Software Corporation.

DOORS is a trademark of Telelogic AB.

InstallShield is a trademark of Macrovision Corporation.

PDF is a trademark of Adobe Corporation USA.

Windows NT, 2000 and XP are trademarks of Microsoft.

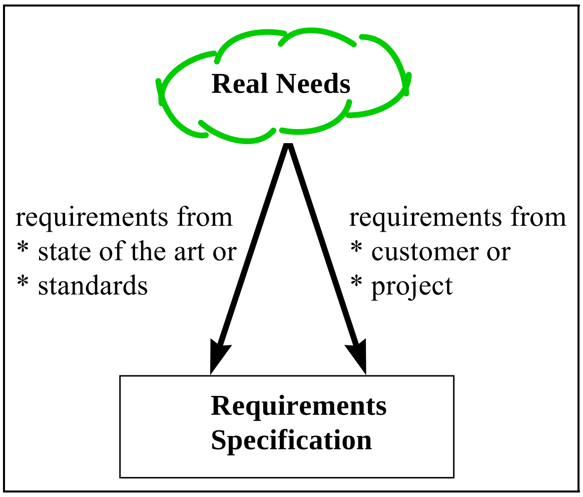
XpdfViewer is a trademark of Glyph & Cog.

CATS Software Tools GmbH would like to thank our UK distributor PhaedruS Systems Ltd for proof reading & editing the English version of this manual. www.phaedsys.org.

CATS Software Tools GmbH thanks the DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE and the IEC International Electrotechnical Commission for permission to reproduce extracts from International Standard IEC 61508.

1 Overview

Prerequisite to produce and certify high quality embedded systems including their software is to know about the functional and non functional requirements imposed on the embedded system. These requirements generally result from two different sources. One source is the specific requirements of the customer or producer e.g. based on their applications or marketing strategy. The other sources are the requirements imposed on the embedded system and its software by the state of the art represented e.g. by national or international standards.

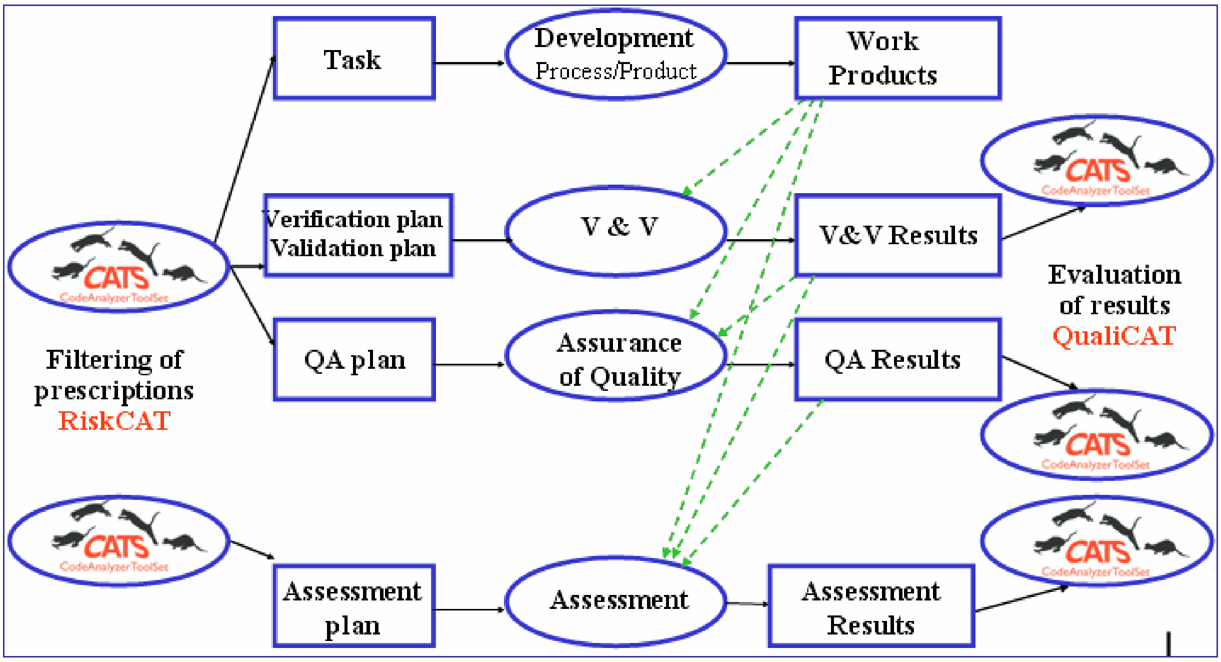


1.1 A suggestion for the efficient handling of standards

<table>
<tr><th colspan="2">For all activities</th></tr>
<tr><td colspan="2">1 Before starting the real work an overview on the considered standard should be achieved. This may be achieved e. g. in technical discussions or in seminars.
2a Selection of the prescriptions from the considered standard relevant for the next working step which needs to be accomplished OR
2b assurance that the standard does not provide guidance for the working step.
3a Generation of a checklist from the selected prescriptions OR
3b transfer of the prescriptions into requirements management.
4 In case relevant prescriptions are not selected for a working step a note about the motivation for omitting the prescription should be made in the checklist respectively the requirements management.
Efficient help for this approach is by RiskCATs.</td></tr>
<tr><th>For the Development of products and processes</th><th>For V&V and QA as well as Assessment of products and processes</th></tr>
<tr><td>5 Taking into account the prescriptions which have been selected</td><td>6 Log compliance with the prescription in the checklist respectively the requirements management (by one sentence) by including a reference on the work product which provides the compliance
Efficient help for this approach is QualiCAT.</td></tr>
</table>

1.2 Usage of RiskCAT

RiskCATs may be used to determine those requirements which shall be applied during process development, development of a whole embedded system or just specific work products, verification & validation, quality assurance, or assessment for purpose of compliance with state of the art given in standards.



1.3 Short description of RiskCAT

RiskCAT is a tool of Code Analyzer Tool Set (CATS) for requirements capturing from standards thereby providing the starting point for high quality development and products in the area of embedded systems and their software. The state of the art in quality of E/E/PES (electrical / electronic / programmable electronic systems) is provided to a large extent by IEC 61508.

The design of RiskCAT is modular and widely configurable. It is possible (for CATS) to adopt the tool to modifications and enhancements of the standards applied as well as the extension to additional standards or other technical rules.

RiskCAT supports

- the determination of the necessary Safety Integrity Level (SIL)
- information about the prescriptions given by IEC 61508
- selection of those prescriptions relevant for the actual step of work
- the export of the selected prescriptions for further work

Besides this RiskCAT offers some support functions.

The work tasks assisted by RiskCAT 61508 are:

1. Determination of the necessary SIL
    - the selection of the normative prescriptions for determination of the necessary SIL,
    - the evaluation of the necessary SIL via the risk reduction needed (for informative purpose only),
    - the evaluation of the necessary SIL via a risk graph (for informative purpose only),
    - the manual SIL selection.

2. Information about prescriptions
    - the structured overview on the prescriptions given by IEC 61508,
    - retrieval in the original standards,
    - the context related presentation of the original standards clause,
    - the context related presentation of explanations to the clause given in IEC 61508 itself (such explanations are available for part of the clauses only),
    - the context related presentation of terms used in the prescription texts given in IEC 61508.

3. Selection of prescriptions
    - the selection of individual prescriptions,
    - the selection of groups of prescriptions according to the degree of obligation,
    - the selection of prescriptions related to documents,
    - the selection of prescriptions related to activities (life cycle phases),
    - the selection of prescriptions related to key words.

4. Comparison of prescriptions at different Quality Levels

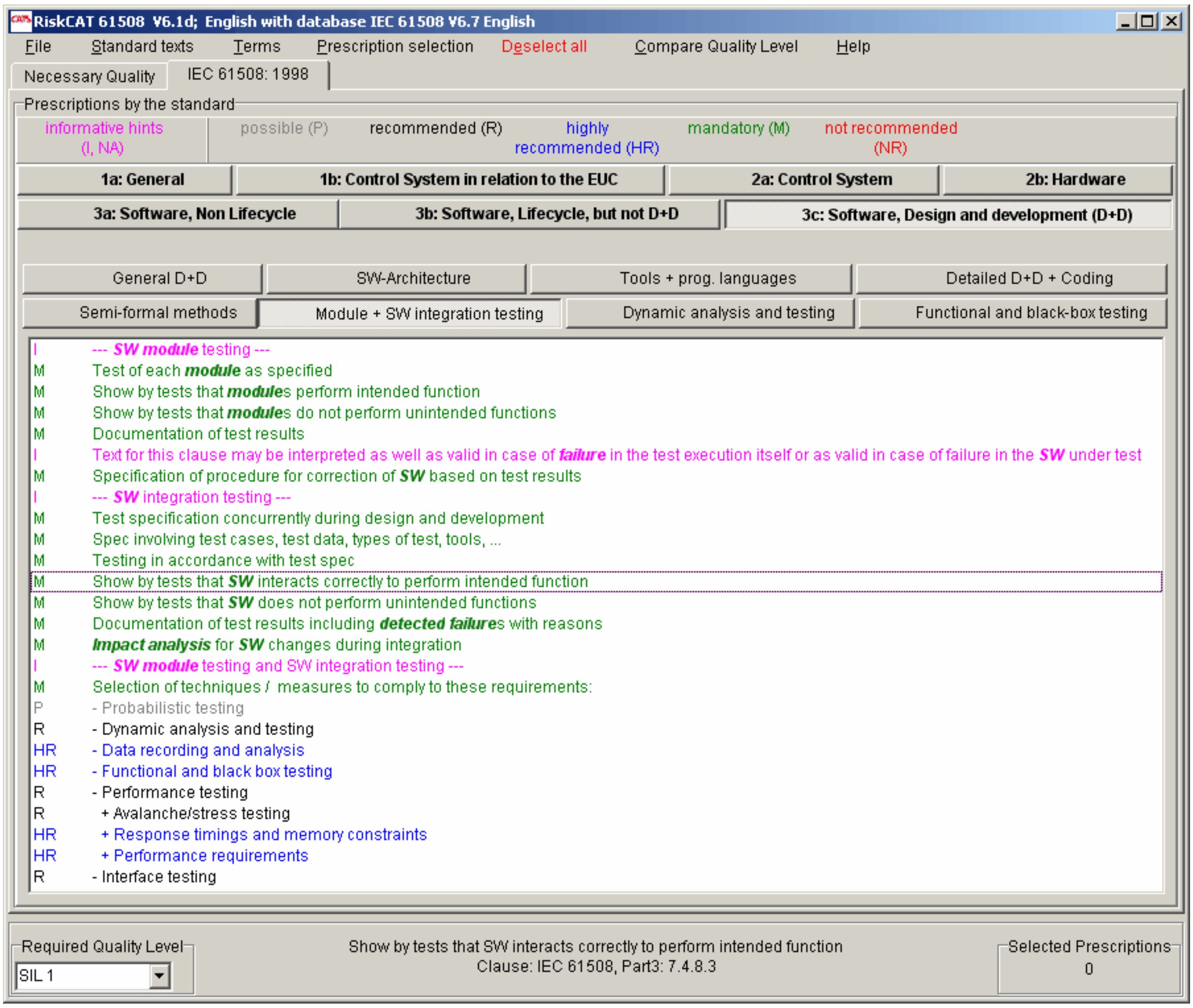
5. Comparison of standard xyz with IEC 61508 (not available with RiskCAT 61508)

6. Export
    - the result storage as simple text file as basis for further processing by the user,
    - the result storage as formatted text file, e.g. as ready checklists or test plans,
    - the result export to ARTiSAN Studio (option at extra expense).
    - the result export to CaliberRM (option at extra expense).
    - the result export to DOORS (option at extra expense),
    - the result export to QualiCAT.

7. Support function
    - editing simple notes for each individual prescription,
    - editing comprehensive notes for each individual prescription,
    - the overview on the terms defined by IEC 61508 which are used by the prescription presentations,
    - the copy function for actually marked prescription into the clipboard,

- the copy function from the standard into the clipboard,
- the storage of prescription profiles as project or company templates in a project file (project storage),
- the reloading of prescription profiles
- on-line help.

An important advantage of the tool supported approach is the possibility to vary interactively risk parameters, risk classes and sets of process and realization prescriptions defining alternative or optimized sets of prescriptions to reach specified quality, safety or reliability targets.


RiskCAT 61508 V6.1d; English with database IEC 61508 V6.7 English
File
Standard texts
Terms
Prescription selection
Deselect all
Compare Quality Level
Help
Necessary Quality
IEC 61508: 1998
Prescriptions by the standard
informative hints (I, NA)
possible (P)
recommended (R)
highly recommended (HR)
mandatory (M)
not recommended (NR)
1a: General
1b: Control System in relation to the EUC
2a: Control System
2b: Hardware
3a: Software, Non Lifecycle
3b: Software, Lifecycle, but not D+D
3c: Software, Design and development (D+D)
General D+D
SW-Architecture
Tools + prog. languages
Detailed D+D + Coding
Semi-formal methods
Module + SW integration testing
Dynamic analysis and testing
Functional and black-box testing

```
I    --- SW module testing ---
M    Test of each module as specified
M    Show by tests that modules perform intended function
M    Show by tests that modules do not perform unintended functions
M    Documentation of test results
I    Text for this clause may be interpreted as well as valid in case of failure in the test execution itself or as valid in case of failure in the SW under test
M    Specification of procedure for correction of SW based on test results
I    --- SW integration testing ---
M    Test specification concurrently during design and development
M    Spec involving test cases, test data, types of test, tools, ...
M    Testing in accordance with test spec
M    Show by tests that SW interacts correctly to perform intended function
M    Show by tests that SW does not perform unintended functions
M    Documentation of test results including detected failures with reasons
M    Impact analysis for SW changes during integration
I    --- SW module testing and SW integration testing ---
M    Selection of techniques / measures to comply to these requirements:
P    - Probabilistic testing
R    - Dynamic analysis and testing
HR   - Data recording and analysis
HR   - Functional and black box testing
R    - Performance testing
R      + Avalanche/stress testing
HR     + Response timings and memory constraints
HR     + Performance requirements
R    - Interface testing
```

Required Quality Level: SIL 1

Show by tests that SW interacts correctly to perform intended function
Clause: IEC 61508, Part3: 7.4.8.3

Selected Prescriptions: 0

Figure 1: RiskCAT 61508 screen

The purpose of RiskCAT 61508 is to assist the user in application of the IEC 61508. However, it is of course not the purpose of the tool to replace the standard. Anyhow the detailed and precise wording of the standards clauses needs to be considered to claim conformance with the standards. RiskCAT’s condensed presentation of the standards contents has been established for the purpose of ease of work, overview and general navigation.

RiskCAT is designed for use by embedded systems software professionals. Experience of using Windows on PCs is required.

2 Installation / First Start / Deinstallation

2.1 The components of RiskCAT

RiskCAT is an application for Windows 2000/ NT/ XP®. It is distributed on an **USB memory stick**.

The **USB memory stick** has the following directory structure:

- RiskCAT_61508 with the subdirectory
  - XPDF
- Tool_Documentation
- CATS_Information
- XPDF_Installation

Besides this the stick optionally contains the installation file for the server disk drive based network installation of RiskCAT

- **setup.exe**[1]

The directory RiskCAT_61508 contains the files:

- The RiskCAT executable **RiskCAT_61508_V61_English.exe**.
- The help file **RiskCAT_61508_V61_English.hlp**.
- The help content file **RiskCAT_61508_V61_English.cnt**.
- The standard files **IEC61508_1_GB_2.pdf**, **IEC61508_2_GB_2.pdf**, **IEC61508_3_GB_2.pdf**, **IEC61508_4_GB_2.pdf** and **IEC61508_7_GB_2.pdf**.

The subdirectory XPDF of directory RiskCAT_61508 contains:

- The XpdfViewer™ ActveX Control, Version 3.0, **XpdfViewerCtrl.ocx**.

The sub-subdirectory t1fonts in the subdirectory XPDF contains:

- The fonts needed by the XpdfViewer

The directory Tool_Documentation contains:

- The product description **RiskCAT_V61_Product.pdf**
- This user manual **RiskCAT_61508_V61_English_UserManual.pdf**

The directory CATS_Information contains:

- Some material about CATS products and courses except of RiskCAT 61508.

The directory XPDF_Installation contains:

- The XpdfViewerCtrl-3[1].00.04.exe (XPDF installer)

[1] This setup is an option supplied with an extra licence only.

Because of licensing conditions the standard files

- **IEC61508_*_GB_*.pdf**

are for use with RiskCAT only.

2.2 Local Operation on a PC

RiskCAT 61508 itself does not need any installation. So just run the executable file **RiskCAT_61508_V61_English.exe** from the directory RiskCAT_61508 on the USB memory stick.

RiskCAT 61508 uses the XpdfViewer™ ActiveX Control which needs installation. This installation is automatically during the first run. Prerequisite for this are administrator rights. Especially for Windows Vista and Windows 7 administrator mode is necessary to run RiskCAT.

For earlier versions of RiskCAT the experience showed that the automatic installation of XpdfViewer™ ActiveX Control sometimes failed. In this case please execute **XpdfViewerCtrl-3[1].00.04.exe** from the directory XPDF_Installation.

CAUTION: The execution of **RiskCAT_61508_V61_English** is possible only from the original USB memory stick. For backup purpose the stick contents may be copied to any backup device. However, RiskCAT_61508_V61_English will operate from the memory stick only.

CAUTION: The first execution of **RiskCAT_61508_V61_English** will install the XpdfViewer™ ActiveX Control, Version 3.0, on the local PC. In case of version conflicts with a XpdfViewer already installed please contact CATS via info@cats-tools.de.

2.3 Uninstallation on a local PC

As RiskCAT does not need any installation so it does neither need any uninstallation.

Uninstallation of XpdfViewer is accomplished by running

WINDOWS-System-Control > Software > Installation/Uninstallation > selecting the XpdfViewer control.

2.4 Network Installation of RiskCAT

RiskCAT offers two different possibilities for network installations:

- You may access RiskCAT_61508_V61_English on the **CATS USB memory stick** network wide or
- you may use a **server disk drive** based installation.

For both types of network installation a single RiskCAT executable is relocated on the server

USB / disk drive. Additionally one XPDF Viewer is installed on each client.

CAUTION: The number of simultaneous usage is limited by the licensed number of users.

The installation procedure for the two installation types differs.

In case of **CATS USB memory stick** usage

- The stick just needs to be connected to the server and
- the local XPDF-Viewer installation needs to be performed by calling the **XpdfViewerCtrl-3[1].00.04.exe** located in the stick directory XPDF_Installation before the first RiskCAT 61508 client session is started.

For a **server disk drive** based installation

- The contents of the CATS USB memory stick (or of the CATS CD) need to be copied into a suitable RiskCAT target directory on the server disk **or**
- the minimum runtime environment for RiskCAT 61508 needs to be to installed on the server by running the **Setup.exe** from the root of the USB memory stick (or of the CATS CD). In this case the XPDF subdirectory must be copied manually into the RiskCAT 61508 target directory created by the Setup.[2]
- As for the USB memory stick usage the local XPDF-Viewer installation needs to be performed by calling the **XpdfViewerCtrl-3[1].00.04.exe** located in the stick directory XPDF_Installation before the first RiskCAT 61508 client session is started.

For the Network Installation the name of the executable should be kept unchanged.

The Network Installation will show just after each start for an instance a black window. This is a necessary behavior. It is no fault.

2.5 Network Uninstallation

The network uninstallation is performed by

- uninstallation of client based XPDF-Viewers by calling **XpdfViewerCtrl-3[1].00.04.exe**

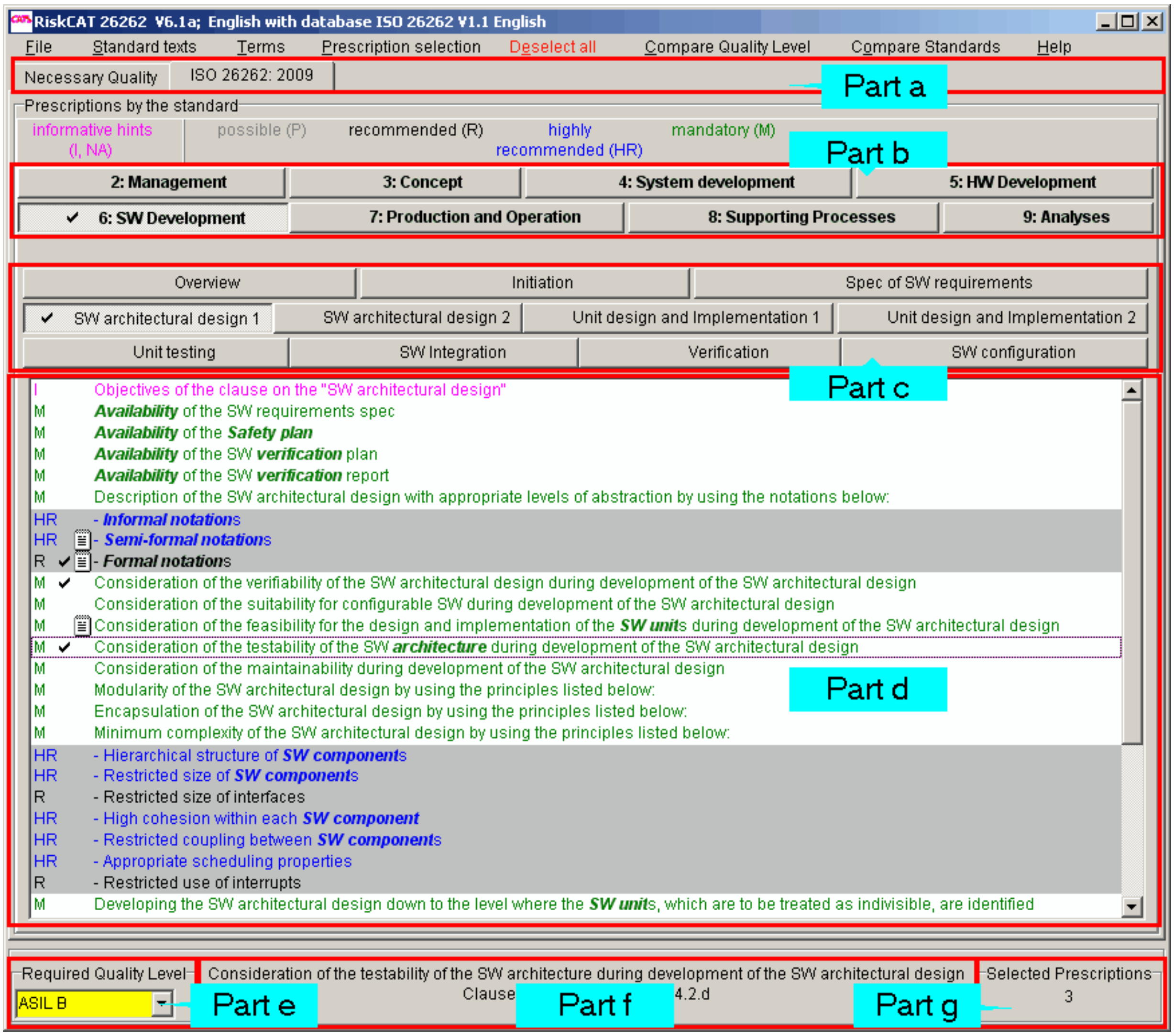
and in case of **server disk drive** based installations additionally by

- deletion of the RiskCAT 61508 components copied on the server **or**
- (in case of having used **Setup.exe** for installation of the minimum runtime environment for RiskCAT 61508 on the server**)** using **WINDOWS system control** or **Setup.exe** to remove the minimum runtime environment for RiskCAT 61508 from the server.

[2] Last installations based on Setup have been in 2006. So this approach would need adoption to the actual environments.

3 Basics

3.1 Screen parts



I Objectives of the clause on the "SW architectural design"
M ***Availability*** of the SW requirements spec
M ***Availability*** of the ***Safety plan***
M ***Availability*** of the SW ***verification*** plan
M ***Availability*** of the SW ***verification*** report
M Description of the SW architectural design with appropriate levels of abstraction by using the notations below:
HR - ***Informal notations***
HR - ***Semi-formal notations***
R ✓ - ***Formal notations***
M ✓ Consideration of the verifiability of the SW architectural design during development of the SW architectural design
M Consideration of the suitability for configurable SW during development of the SW architectural design
M Consideration of the feasibility for the design and implementation of the ***SW units*** during development of the SW architectural design
M ✓ Consideration of the testability of the SW ***architecture*** during development of the SW architectural design
M Consideration of the maintainability during development of the SW architectural design
M Modularity of the SW architectural design by using the principles listed below:
M Encapsulation of the SW architectural design by using the principles listed below:
M Minimum complexity of the SW architectural design by using the principles listed below:
HR - Hierarchical structure of ***SW components***
HR - Restricted size of ***SW components***
R - Restricted size of interfaces
HR - High cohesion within each ***SW component***
HR - Restricted coupling between ***SW components***
HR - Appropriate scheduling properties
R - Restricted use of interrupts
M Developing the SW architectural design down to the level where the ***SW units***, which are to be treated as indivisible, are identified

Required Quality Level: ASIL B

Consideration of the testability of the SW architecture during development of the SW architectural design
Clause 4.2.d

Selected Prescriptions: 3

Figure 2: RiskCAT screen parts

a: Task tabs
b: Area tabs
c: Topic tabs
d: Prescription window
e: SIL corner
f: Information line
g: Counter corner

3.2 Interrelationship between the screen parts

The screen parts b, c and d are used to present the prescriptions.

The Safety Integrity Level (SIL) selected in the SIL corner (screen part e) controls the degree of obligation of the prescriptions given in screen part d.

3.3 Prescription states

RiskCAT presents the individual requirements in the Prescription window (screen part d) including their state. The three state dimensions are

- marked / unmarked
- selected / deselected
- with comment / without comment

The state "marked" may be assigned to one prescription only at any time. Marking of a prescription is by a single left mouse button click. It is visible by a box around the text describing the prescription.

The state "selected" may be assigned to one, several or even all prescriptions at the same time. Manual election of a prescription is by a single left mouse button click. It is visible by a tick ✓ left of the text describing the prescription. Automatic selection is discussed later in this manual (see chapters 6.3, "Selection of groups of prescriptions according to the degree of obligation", to 6.6, "Selection of prescriptions related to key words").

The state "with comment" may be assigned to one, several or even all prescriptions at the same time. Adding comments to a prescription is via context menu (depress of right mouse button) in the prescription list boxes. It is visible by a ▤ left of the text describing the prescription.

3.4 Prescription colours

The prescriptions in the Prescription window (screen part d) are dynamically coloured. The colour depends on the degree of obligation which may be influenced by the SIL selected in the SIL corner (screen area b). Usage is made of Informative (pink), Possible (grey), Highly recommended (blue), and Mandatory (green).

For those users who may be colour blind or for usage with certain beamers the degree of obligation is given in the Prescription window by characters left besides the prescription text in addition to the colour.

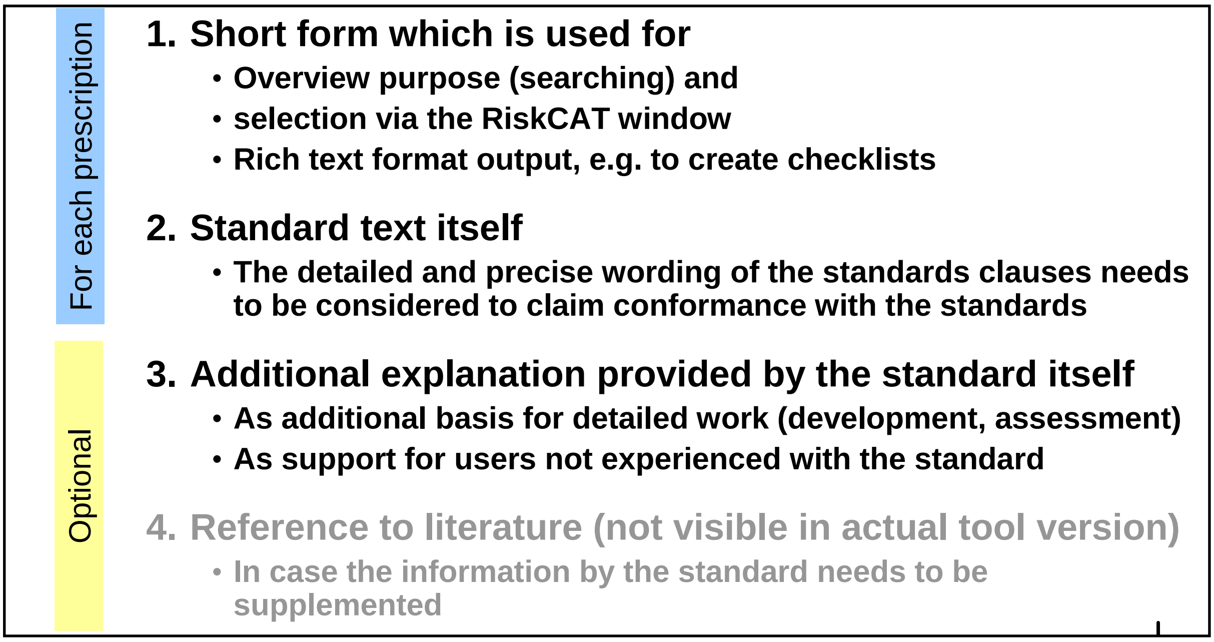
3.5 Structure of the prescriptions presentation used with RiskCAT

RiskCAT starts from standards. So the original sets of prescriptions are the **standards** represented by the task tabs (screen part a).

A standard may consist of different parts as e.g. IEC 61508 which has 7 parts. The standard or even its parts may be such voluminous that it is not appropriate to use all prescriptions as an entity. This has been the reason to break down some standards into **areas** represented by the area tabs (screen part b). Depending on the standard an area may consist of a part of a standard, some clauses of a standard or some clauses of a part of a standard. For details see chapter **Fehler! Verweisquelle konnte nicht gefunden werden.** of this manual.

Most standards cover a variety of **topics** represented by the topic tabs (screen part c). The approach has been to have an assignment between standards chapters and RiskCAT topics. However, in some cases standard chapters have been further split up, because of a high number of prescriptions or because of different matters covered in the same chapter.

A further structuring is by grey shaded areas in the prescription window. This presentation indicates that the marked requirements are alternatives to each other.



1. **Short form which is used for**
   - **Overview purpose (searching) and**
   - **selection via the RiskCAT window**
   - **Rich text format output, e.g. to create checklists**
2. **Standard text itself**
   - **The detailed and precise wording of the standards clauses needs to be considered to claim conformance with the standards**
3. **Additional explanation provided by the standard itself**
   - **As additional basis for detailed work (development, assessment)**
   - **As support for users not experienced with the standard**
4. **Reference to literature (not visible in actual tool version)**
   - **In case the information by the standard needs to be supplemented**

Figure 3: Presentation of the standard clauses in four levels

4 Determination of the necessary SIL

Practical experience shows that at determination of the necessary Safety Integrity Level difference is not made between

- The **normative** prescriptions of the IEC 61508
  They may be found in part 1 and state the border conditions for the determination of the necessary SIL. Their disadvantage is the impossibility to determine for a certain task the right SIL in a simple manner.
  However, this is not surprising because the determination of the SIL – and by this determination of the tolerable risk – is a social / political / legal decision which may be different in different countries as well as for different industries.
- The **informative** explanations of the IEC 61508
  They may be found in part 5 and allow in a straight forward way to determine the SIL necessary for a certain task.
  They are useful for a first orientation. But it is strongly advised not to use these explanations for the decision about tolerable number of injured persons, environmental or material damage.

The normative prescriptions for the determination of the necessary SIL may be selected with RiskCAT in a simple way – as well as other prescriptions. Please refer for this purpose to chapter "5 Information about the prescriptions".

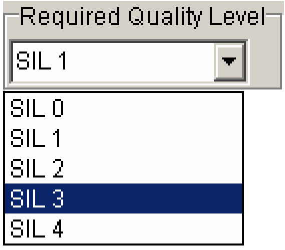
This chapter addresses two possibilities for orientation about the necessary SIL which are given by IEC 61508, part 5. They are provided via the task tab "Necessary Quality". The determination of risk parameters may be with one of the two approaches

- Reducing of the risk to a tolerable level or
- Risk Graph

For Details about the approaches see chapter "13.4 About the Safety Integrity Level (SIL)" of this manual.

CAUTION: The approaches described here being implemented on the informative part 5 of IEC 61508 are not applicable for the binding determination of the necessary SIL.
During recent years they have been used – especially in Germany – for a first orientation.

4.1 Manual selection of the Safety Integrity Level



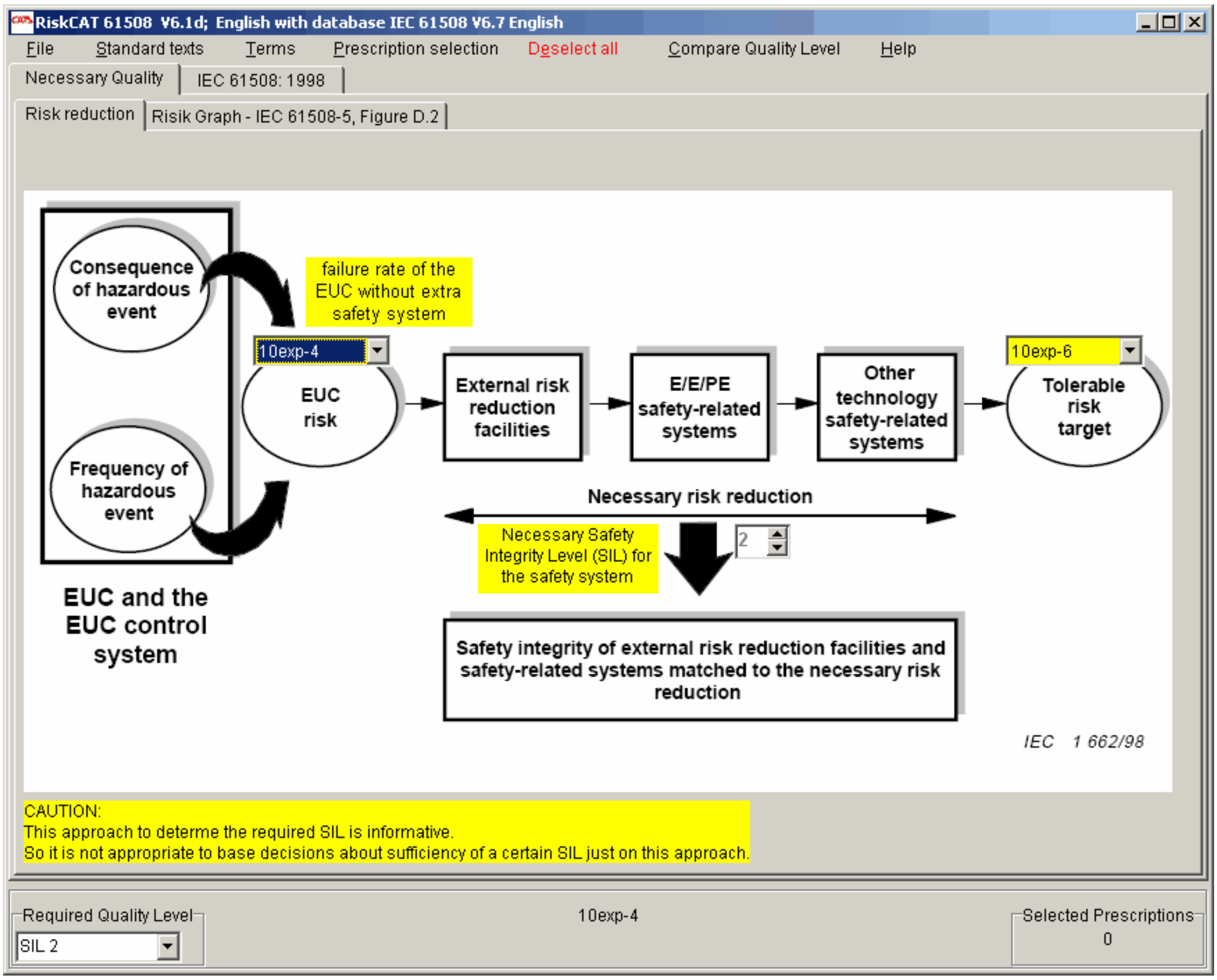
Required Quality Level
SIL 1

The Safety Integrity Level (SIL) may be manually selected in the SIL corner.

The selected SIL is used to determine the degree of obligation of the IEC 61508 prescriptions.

4.2 SIL determination via the necessary risk reduction

This approach is activated by selecting the RiskCAT task tab “Necessary Quality” followed by “Risk reduction”. The approach is based on IEC 61508, part 5, figure C.1.


RiskCAT 61508 V6.1d; English with database IEC 61508 V6.7 English
File
Standard texts
Terms
Prescription selection
Deselect all
Compare Quality Level
Help
Necessary Quality
IEC 61508: 1998
Risk reduction
Risik Graph - IEC 61508-5, Figure D.2
Consequence of hazardous event
Frequency of hazardous event
EUC and the EUC control system
failure rate of the EUC without extra safety system
EUC risk
External risk reduction facilities
E/E/PE safety-related systems
Other technology safety-related systems
Tolerable risk target
Necessary risk reduction
Necessary Safety Integrity Level (SIL) for the safety system
Safety integrity of external risk reduction facilities and safety-related systems matched to the necessary risk reduction
IEC 1 662/98

failure rate of the EUC without extra safety system: 10exp-4

Tolerable risk target: 10exp-6

Necessary Safety Integrity Level (SIL) for the safety system: 2

CAUTION:
This approach to determe the required SIL is informative.
So it is not appropriate to base decisions about sufficiency of a certain SIL just on this approach.

Required Quality Level: SIL 2

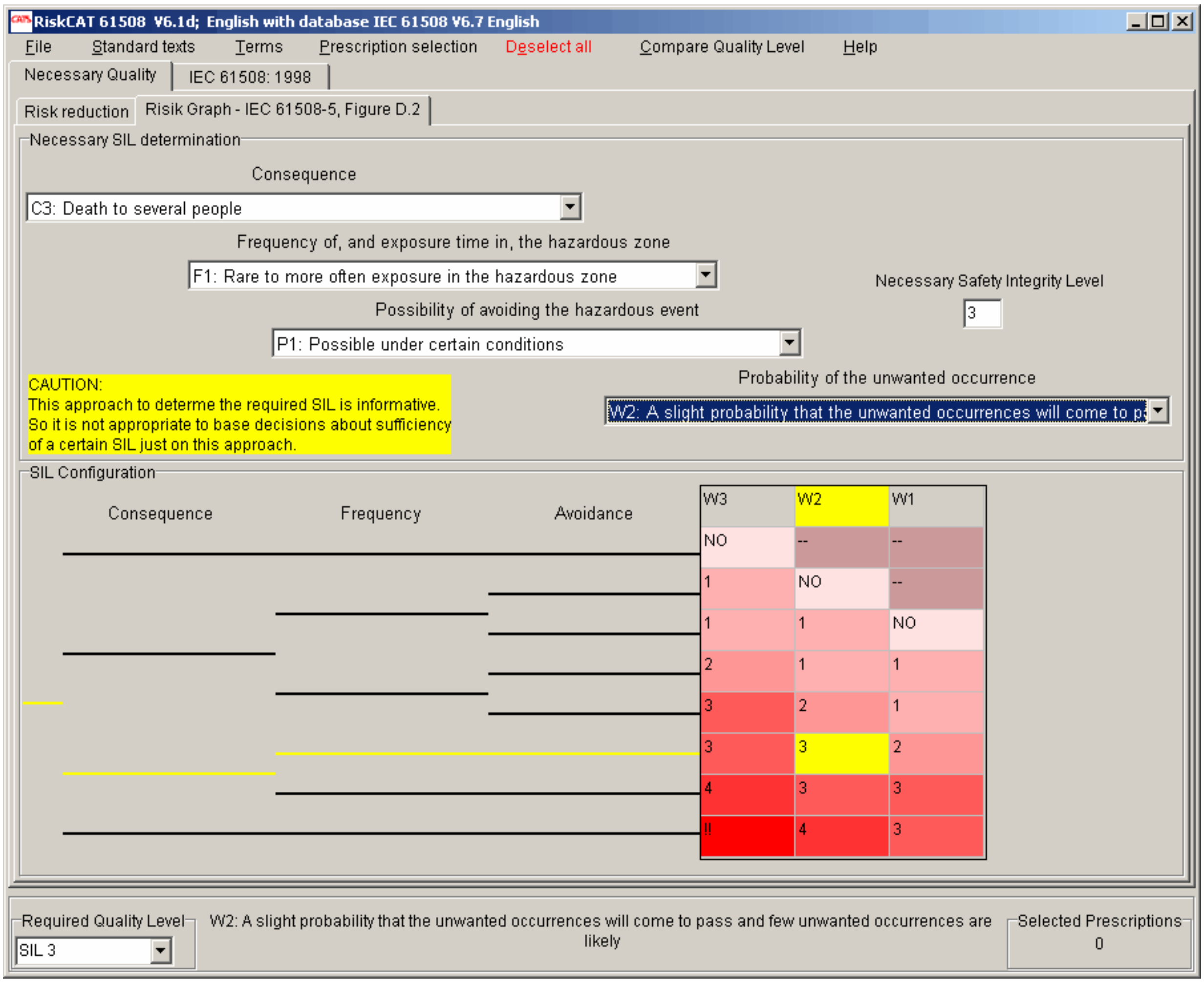
10exp-4

Selected Prescriptions: 0

After changing “failure rate of the EUC (Equipment under control) without extra safety system” or “Tolerable risk target” the Safety Integrity Level is calculated automatically. After changes the SIL is transferred to the SIL corner (screen part e). The value shown in the SIL corner may be changed manually.

4.3 SIL determination via a risk graph

This approach is activated by selecting the RiskCAT task tab “Necessary Quality” followed by “Risk Graph”. The approach is based on IEC 61508, part 5, figure D.2 and table D.1.



Consequence: C3: Death to several people

Frequency of, and exposure time in, the hazardous zone: F1: Rare to more often exposure in the hazardous zone

Possibility of avoiding the hazardous event: P1: Possible under certain conditions

Necessary Safety Integrity Level: 3

Probability of the unwanted occurrence: W2: A slight probability that the unwanted occurrences will come to p

CAUTION:
This approach to determe the required SIL is informative.
So it is not appropriate to base decisions about sufficiency of a certain SIL just on this approach.

W3	W2	W1
NO	--	--
1	NO	--
1	1	NO
2	1	1
3	2	1
3	3	2
4	3	3
!!	4	3

Required Quality Level: SIL 3

W2: A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely

Selected Prescriptions: 0

The complete text of the selected risk parameter is displayed in the information line (screen part f).

After changing a risk parameter the Safety Integrity Level is calculated automatically. After changes the SIL is transferred to the SIL corner (screen part e). The value shown in the SIL corner may be changed manually.

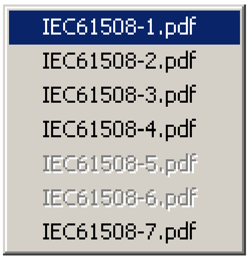
CAUTION: Please note that IEC 61508, part 5, presents by **figure D.1** another Risk Graph which is different.

5 Information about the prescriptions

5.1 Structured overview on the recommended prescriptions

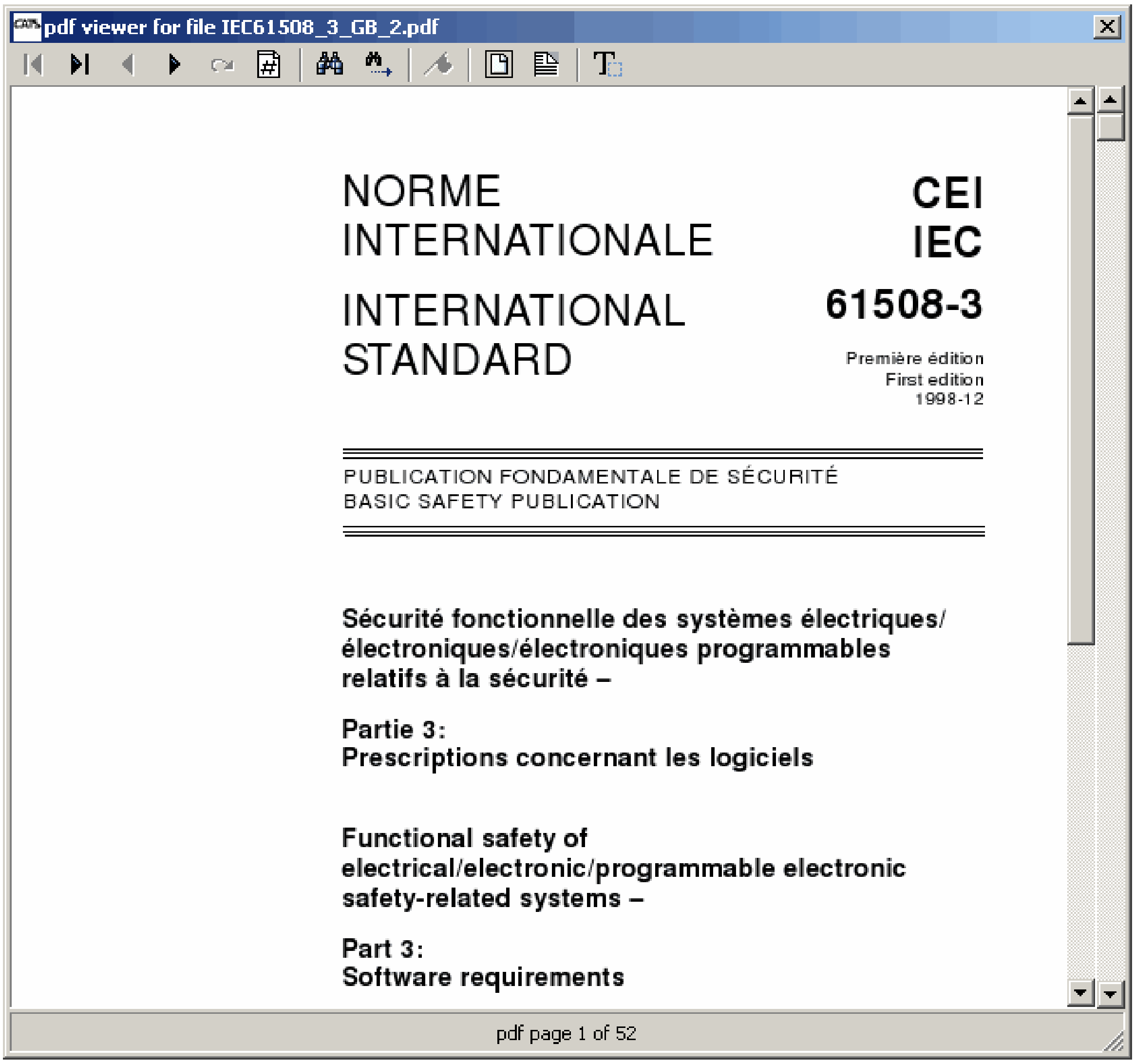
Each of the area tabs represents an important theme within the scope of embedded controllers and their software. And each of the topic tabs represents a coherent set of prescriptions. Just by selection of corresponding tabs RiskCAT provides an overview about the prescriptions with respect to the topic given as tab text.

5.2 Retrieval in the original standards



RiskCAT offers an interface for viewing the original standards via the XpdfViewer™ XpdfViewerCtrl.ocx library.

Retrieval is started via “Standard texts“ menu.



NORME INTERNATIONALE

CEI IEC

INTERNATIONAL STANDARD

61508-3

Première édition
First edition
1998-12

PUBLICATION FONDAMENTALE DE SÉCURITÉ
BASIC SAFETY PUBLICATION

Sécurité fonctionnelle des systèmes électriques/ électroniques/électroniques programmables relatifs à la sécurité –

Partie 3:
Prescriptions concernant les logiciels

Functional safety of electrical/electronic/programmable electronic safety-related systems –

Part 3:
Software requirements

The size of the standards window may be changed by positioning the mouse on the windows border (preferred on the left or right hand side) followed by pressing the left mouse button and then moving it.

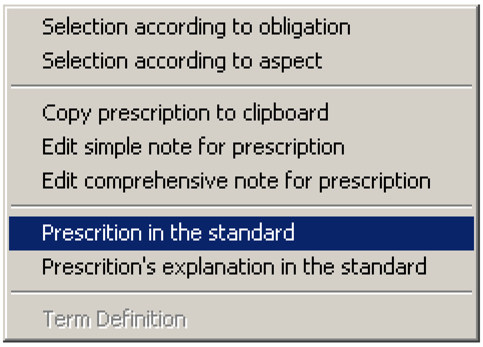
The XpdfViewer™ provides the following functions:

- First page
- Last page
- Previous page
- Next page
- Go to page
- Find
- Find next
- Adjust to page height
- Adjust to page width
- Copy text to clipboard
  (see as well chapter "10.4 Copying from the standards into the clipboard")

5.3 Context related retrieval in the original standards

Besides the interface for full text browsing RiskCAT offers an interface for context sensitive browsing in original standards.

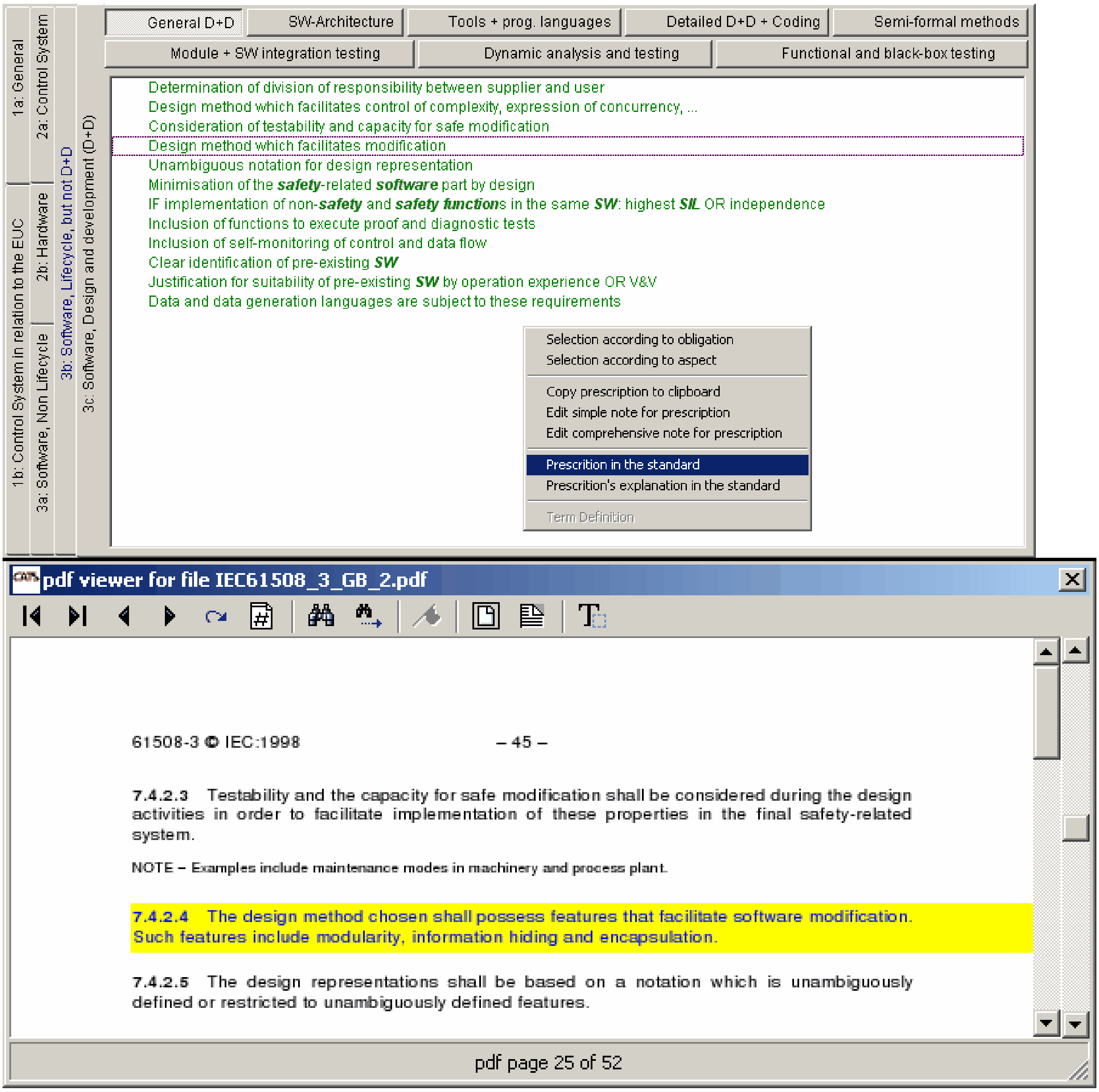
The context related retrieval is activated via context menu in the prescription window (screen part d in Figure 2).


Selection according to obligation
Selection according to aspect
Copy prescription to clipboard
Edit simple note for prescription
Edit comprehensive note for prescription
Prescrition in the standard
Prescrition's explanation in the standard
Term Definition

The steps are:

- Mark the prescription establishing the context by a single left mouse button click. (Otherwise the page selected by context related retrieval is somewhat arbitrary.)
- Activate context menu (depress right mouse button while the pointer is in the prescription window)
- Choose "Prescription in the standard"

RiskCAT will show the page of the standard highlighting the clause in context. The size of the standards window may be changed by positioning the mouse on the windows border (preferred on the left or right hand side) followed by pressing the left mouse button and then moving it.


1a: General
2a: Control System
1b: Control System in relation to the EUC
2b: Hardware
3a: Software, Non Lifecycle
3b: Software, Lifecycle, but not D+D
3c: Software, Design and development (D+D)
General D+D
SW-Architecture
Tools + prog. languages
Detailed D+D + Coding
Semi-formal methods
Module + SW integration testing
Dynamic analysis and testing
Functional and black-box testing
Selection according to obligation
Selection according to aspect
Copy prescription to clipboard
Edit simple note for prescription
Edit comprehensive note for prescription
Prescrition in the standard
Prescrition's explanation in the standard
Term Definition
pdf viewer for file IEC61508_3_GB_2.pdf
pdf page 25 of 52

Determination of division of responsibility between supplier and user
Design method which facilitates control of complexity, expression of concurrency, ...
Consideration of testability and capacity for safe modification
Design method which facilitates modification
Unambiguous notation for design representation
Minimisation of the ***safety***-related ***software*** part by design
IF implementation of non-***safety*** and ***safety functions*** in the same ***SW***: highest ***SIL*** OR independence
Inclusion of functions to execute proof and diagnostic tests
Inclusion of self-monitoring of control and data flow
Clear identification of pre-existing ***SW***
Justification for suitability of pre-existing ***SW*** by operation experience OR V&V
Data and data generation languages are subject to these requirements

61508-3 © IEC:1998 – 45 –

7.4.2.3 Testability and the capacity for safe modification shall be considered during the design activities in order to facilitate implementation of these properties in the final safety-related system.

NOTE – Examples include maintenance modes in machinery and process plant.

7.4.2.4 The design method chosen shall possess features that facilitate software modification. Such features include modularity, information hiding and encapsulation.

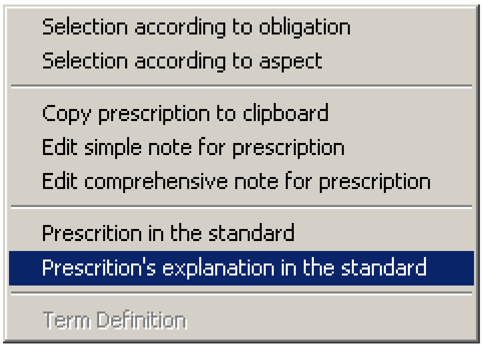
7.4.2.5 The design representations shall be based on a notation which is unambiguously defined or restricted to unambiguously defined features.

If other PDF versions of the standards have been installed than those supplied by CATS, RiskCAT may show the wrong page and may highlight the wrong clause. Therefore only those standards supplied by CATS should be used with the RiskCAT tools.

5.4 The context related presentation of explanations to the clause provided by IEC 61508 itself

For certain clauses IEC 61508 itself provides additional explanations, mostly from part 7 of the standard. RiskCAT offers an interface for context sensitive browsing the explanations from the original standard.

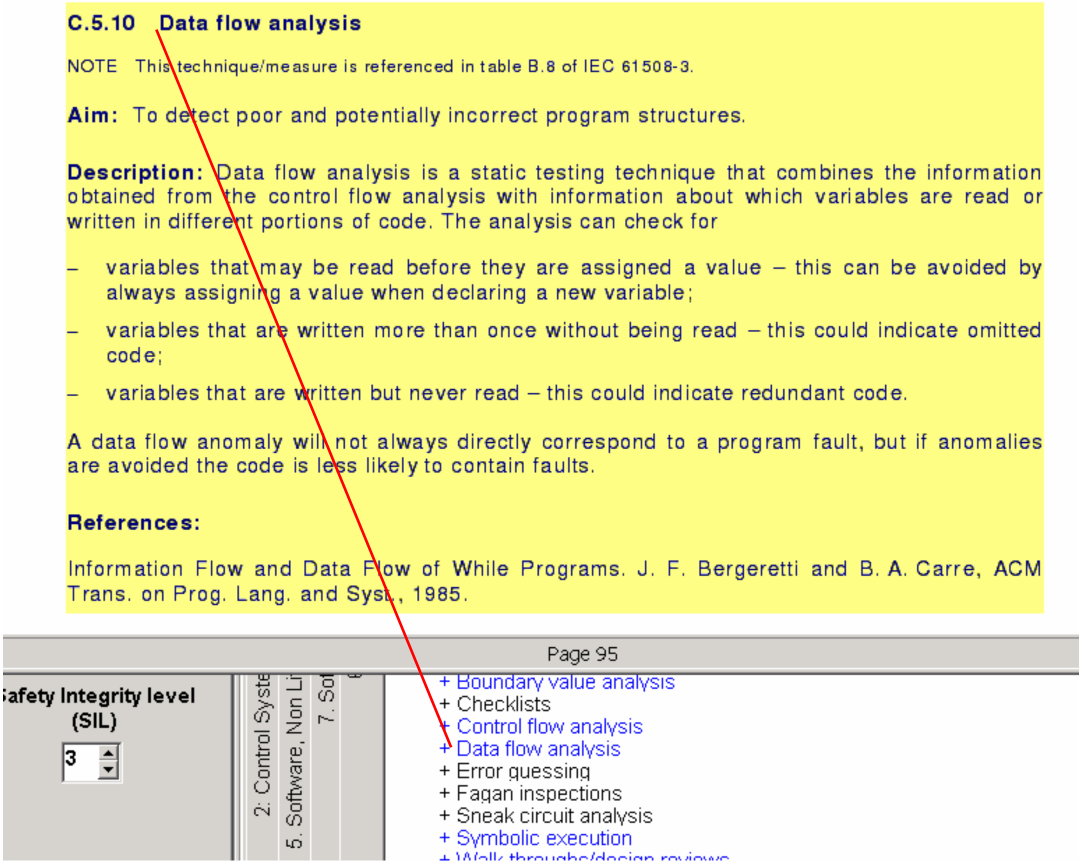
The context related explanation is activated via context menu in the prescription window.


Selection according to obligation
Selection according to aspect
Copy prescription to clipboard
Edit simple note for prescription
Edit comprehensive note for prescription
Prescrition in the standard
Prescrition's explanation in the standard
Term Definition

The steps are:

- Mark the prescription establishing the context by a single left mouse button click. (Otherwise the page selected by context related retrieval is somewhat arbitrary.)
- Activate context menu (depress right mouse button while the pointer is in the prescription window)
- Choose "Prescription's explanation in the standard"

RiskCAT will show the page of the standard highlighting the explanation in context. The size of the standards window may be changed by positioning the mouse on the windows border (preferred on the left or right hand side) followed by pressing the left mouse button and then moving it.



C.5.10 Data flow analysis

NOTE This technique/measure is referenced in table B.8 of IEC 61508-3.

Aim: To detect poor and potentially incorrect program structures.

Description: Data flow analysis is a static testing technique that combines the information obtained from the control flow analysis with information about which variables are read or written in different portions of code. The analysis can check for

– variables that may be read before they are assigned a value – this can be avoided by always assigning a value when declaring a new variable;

– variables that are written more than once without being read – this could indicate omitted code;

– variables that are written but never read – this could indicate redundant code.

A data flow anomaly will not always directly correspond to a program fault, but if anomalies are avoided the code is less likely to contain faults.

References:

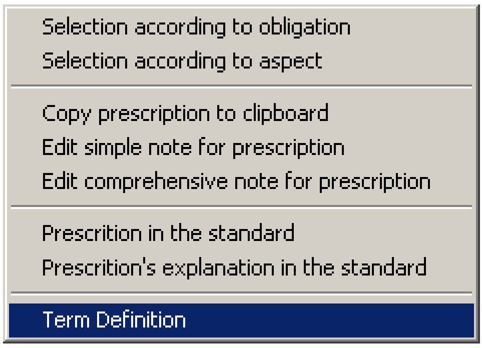
Information Flow and Data Flow of While Programs. J. F. Bergeretti and B. A. Carre, ACM Trans. on Prog. Lang. and Syst., 1985.

If other PDF versions of the standards have been installed than those supplied by CATS, RiskCAT may show the wrong page and may highlight the wrong clause. Therefore only those standards supplied by CATS should be used with the RiskCAT tools.

5.5 The context related presentation of terms used in the prescription texts given in IEC 61508

For certain terms IEC 61508 part 4 provides definitions. RiskCAT provides an interface for context sensitive browsing the definitions from the original standard. The defined terms used in the prescription's presentation are presented in bold.

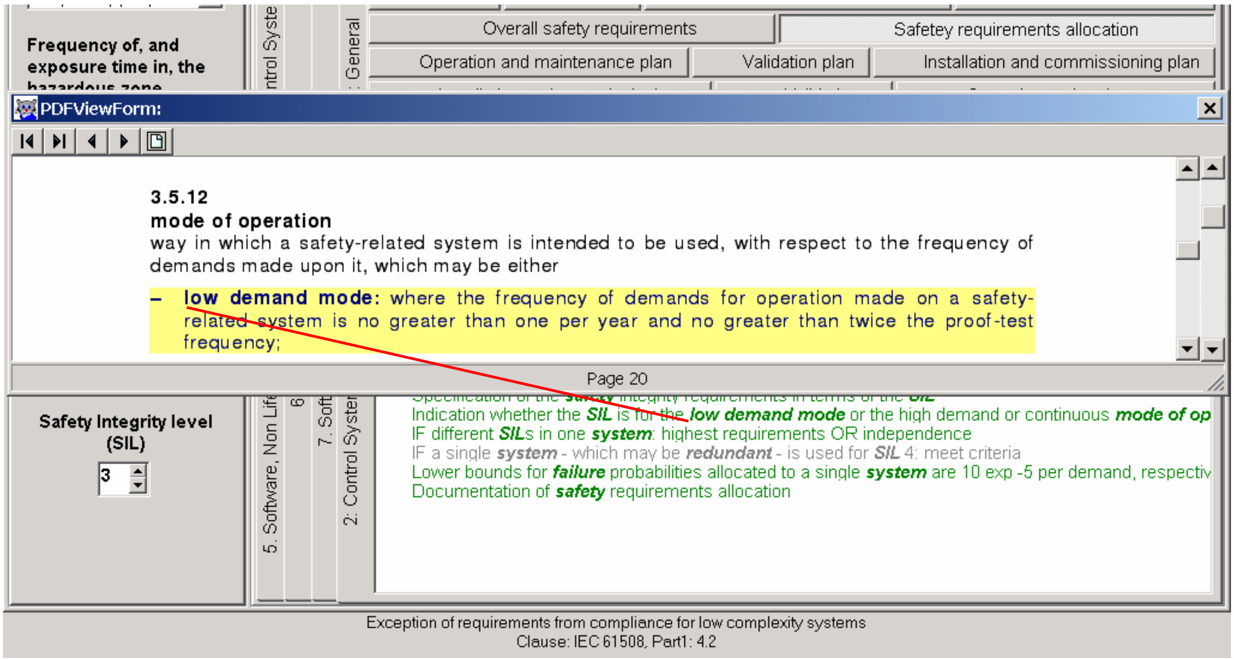
The context related term definition is activated via context menu in the prescription window.


Selection according to obligation
Selection according to aspect
Copy prescription to clipboard
Edit simple note for prescription
Edit comprehensive note for prescription
Prescrition in the standard
Prescrition's explanation in the standard
Term Definition

The steps are:

- Go with the cursor to a defined (**bold**) term. The type of the cursor which normally is ↖ then will change to ☝
- Activate context menu (depress right mouse button while the pointer is in the prescription window)
- Choose "Term Definition"

RiskCAT will show the page of the standard highlighting the definition in context. The size of the standards window may be changed by positioning the mouse on the windows border (preferred on the left or right hand side) followed by pressing the left mouse button and then moving it.


Frequency of, and exposure time in, the hazardous zone
ntrol Syste
: General
Overall safety requirements
Safetey requirements allocation
Operation and maintenance plan
Validation plan
Installation and commissioning plan
PDFViewForm:
Page 20
Safety Integrity level (SIL)
3
5. Software, Non Life
6
7. Soft
2: Control Syster

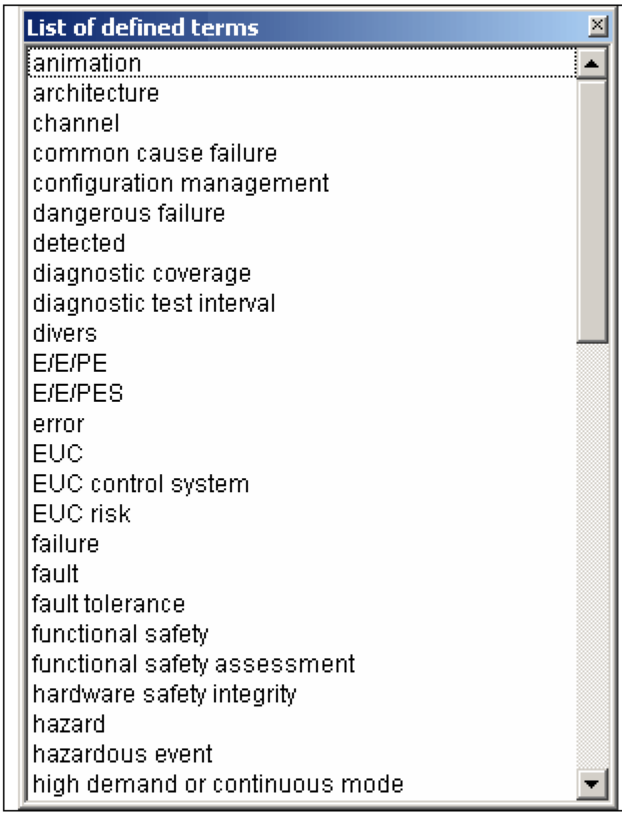
3.5.12
mode of operation
way in which a safety-related system is intended to be used, with respect to the frequency of demands made upon it, which may be either

– **low demand mode:** where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof-test frequency;

Specification of the ***safety*** integrity requirements in terms of the ***SIL***
Indication whether the ***SIL*** is for the ***low demand mode*** or the high demand or continuous ***mode of op***
IF different ***SIL***s in one ***system***: highest requirements OR independence
IF a single ***system*** - which may be ***redundant*** - is used for ***SIL*** 4: meet criteria
Lower bounds for ***failure*** probabilities allocated to a single ***system*** are 10 exp -5 per demand, respectiv
Documentation of ***safety*** requirements allocation

Exception of requirements from compliance for low complexity systems
Clause: IEC 61508, Part1: 4.2

If other PDF versions of the standards have been installed than those supplied by CATS RiskCAT may show the wrong page and may highlight the wrong clause. Therefore only those standards supplied by CATS should be used with the RiskCAT tools.



List of defined terms

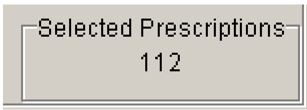
animation
architecture
channel
common cause failure
configuration management
dangerous failure
detected
diagnostic coverage
diagnostic test interval
divers
E/E/PE
E/E/PES
error
EUC
EUC control system
EUC risk
failure
fault
fault tolerance
functional safety
functional safety assessment
hardware safety integrity
hazard
hazardous event
high demand or continuous mode

Browsing of terms is possible as well independently from the prescription's context via the “Terms” menu. The window shown aside presents the terms in alphabetic order.

By double click on a term in the list the term definition is displayed.

6 Selection of prescriptions

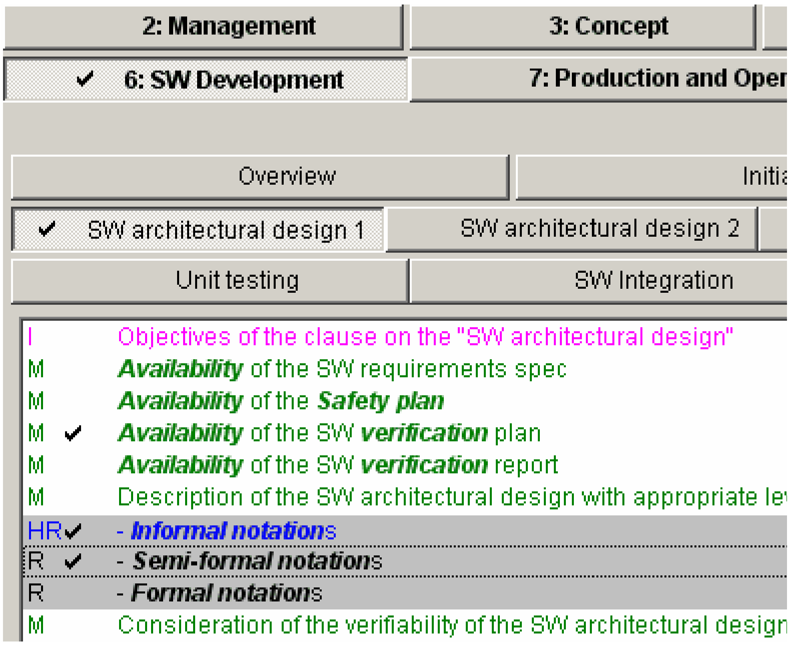
6.1 The number of selected prescriptions



Selected Prescriptions
112

Starting with version 5.9a RiskCAT shows in the Counter Corner (screen part g) the number of selected prescriptions.

6.2 Selection of individual prescriptions



2: Management | 3: Concept
✓ 6: SW Development | 7: Production and Oper
Overview | Initi
✓ SW architectural design 1 | SW architectural design 2
Unit testing | SW Integration

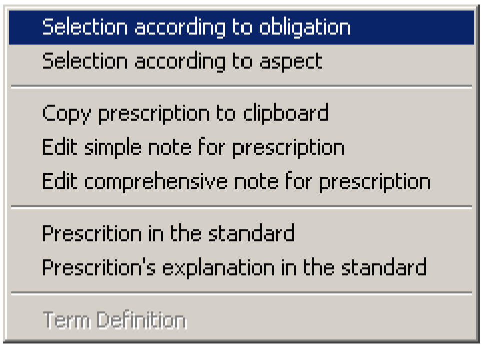
I Objectives of the clause on the "SW architectural design"
M ***Availability*** of the SW requirements spec
M ***Availability*** of the ***Safety plan***
M ✓ ***Availability*** of the SW ***verification*** plan
M ***Availability*** of the SW ***verification*** report
M Description of the SW architectural design with appropriate le
HR ✓ - ***Informal notations***
R ✓ - ***Semi-formal notations***
R - ***Formal notations***
M Consideration of the verifiability of the SW architectural design

Individual prescriptions are selected / deselected by a double click with left mouse button. Selection is visible by

- a check mark ✓ to the left of the prescription itself
- a check mark ✓ to the left of the corresponding topic tab
- a check mark ✓ to the left of the corresponding area tab

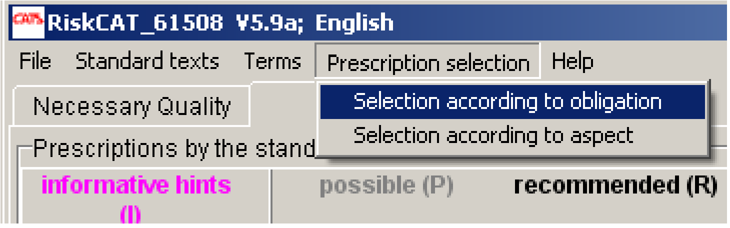
The selection is in addition to already selected prescriptions. If the real interest is just to concentrate on the prescriptions actually selected; precautions need to be applied to de-select any prescriptions that may have been selected previously. (The selection / de-selection of several prescriptions is described in next chapter of this manual.)

6.3 Selection of groups of prescriptions according to the degree of obligation

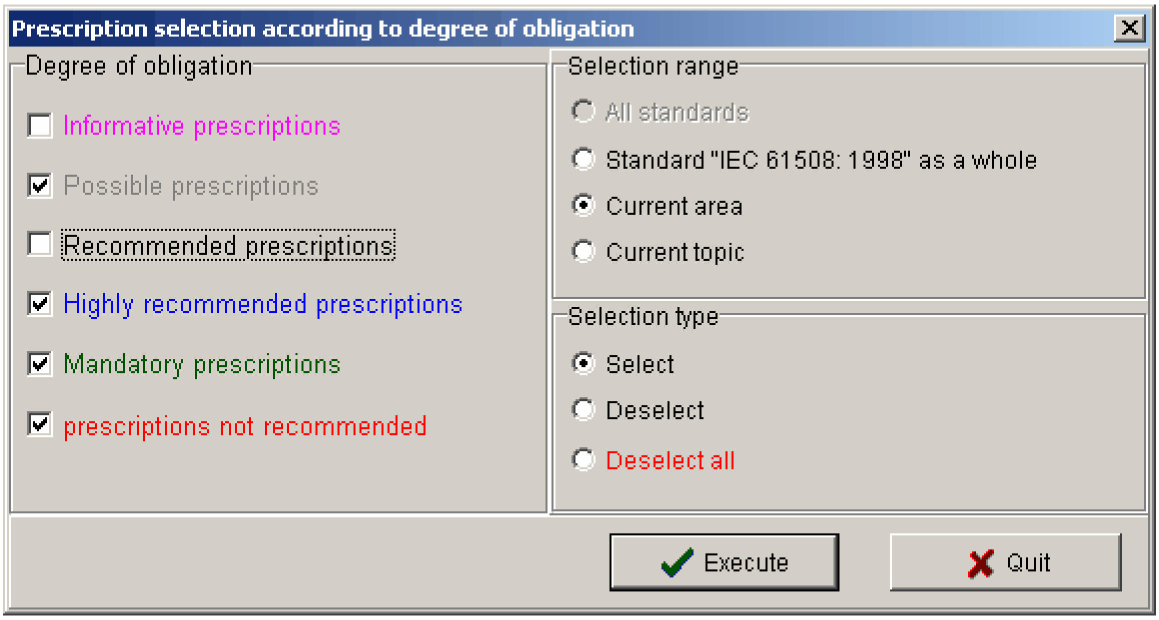

Selection according to obligation
Selection according to aspect
Copy prescription to clipboard
Edit simple note for prescription
Edit comprehensive note for prescription
Prescrition in the standard
Prescrition's explanation in the standard
Term Definition

The selection of groups according to the degree of obligation[3] – under the currently selected SIL – of the prescriptions is activated via

- the context menu (depress right mouse button while the pointer is in the prescription window (screen part d in Figure 2)) or
- via the menu "Prescription selection"


RiskCAT_61508 V5.9a; English
File
Standard texts
Terms
Prescription selection
Help
Selection according to obligation
Selection according to aspect
Necessary Quality
Prescriptions by the stand
informative hints (I)
possible (P)
recommended (R)

After a single click on "Selection according to obligation" the selection form shown below will appear.


Prescription selection according to degree of obligation

Degree of obligation

☐ Informative prescriptions

☑ Possible prescriptions

☐ Recommended prescriptions

☑ Highly recommended prescriptions

☑ Mandatory prescriptions

☑ prescriptions not recommended

Selection range

○ All standards

○ Standard "IEC 61508: 1998" as a whole

● Current area

○ Current topic

Selection type

● Select

○ Deselect

○ Deselect all

If the "Standard … as a whole" is activated the selection will be for all prescriptions in all areas for all topics.

If "Current area" is activated the selection will be for all topics in the active area. The visibility of the selection is same as for individual prescriptions selection.

[3] For the degree of obligation please refer as well to chapter 13.2, "Presentation of the degree of obligation of the requirements".

If "Current topic" is activated the selection will be just for the prescriptions in active topic. The visibility of the selection is same as for individual prescriptions selection.

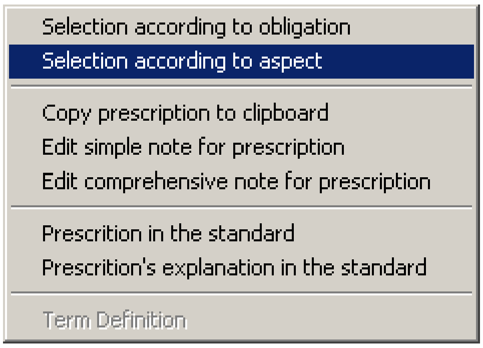
CAUTION: If the SIL is changed between group selection and the "Deselect" the set of deselected prescriptions may be different from the selected set. So here "DeSelect" is only the inverse function to "Select" if SIL is the same for both actions.

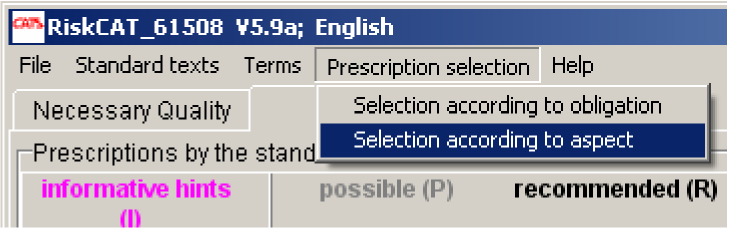
The selection is in addition to already selected prescriptions. If the real interest is just to concentrate on the prescriptions you are about to select then precautions need to be applied that at starting prescription selection no prescriptions are already selected.

Example for the usage of selection of groups of prescriptions:

> IEC 61508 in certain places explicitly mentions that certain solutions are "possible". Key word in the standard is "may".
>
> If you doubt whether you may allocate a safety function across more than one safety-related system you should select all possible prescriptions and check them afterwards.

6.4 Selection of prescriptions related to documents

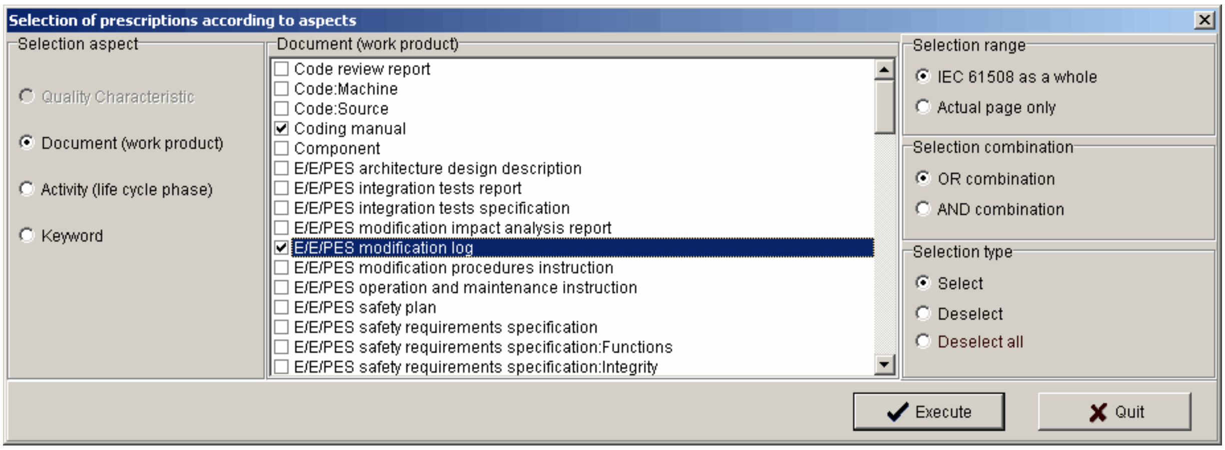

Selection according to obligation
Selection according to aspect
Copy prescription to clipboard
Edit simple note for prescription
Edit comprehensive note for prescription
Prescrition in the standard
Prescrition's explanation in the standard
Term Definition


RiskCAT_61508 V5.9a; English
File
Standard texts
Terms
Prescription selection
Help
Necessary Quality
Selection according to obligation
Selection according to aspect
Prescriptions by the stand
informative hints (I)
possible (P)
recommended (R)

The selection of groups of prescriptions according to documents is activated via

- the context menu (depress right mouse button while the pointer is in the prescription window (screen part d in Figure 2)) or
- via the menu "Prescription selection"

After a single click on "Selection according to aspect" the selection form shown below will appear.



Selection of prescriptions according to aspects

Selection aspect
- ○ Quality Characteristic
- ● Document (work product)
- ○ Activity (life cycle phase)
- ○ Keyword

Document (work product)
- □ Code review report
- □ Code:Machine
- □ Code:Source
- ☑ Coding manual
- □ Component
- □ E/E/PES architecture design description
- □ E/E/PES integration tests report
- □ E/E/PES integration tests specification
- □ E/E/PES modification impact analysis report
- ☑ E/E/PES modification log
- □ E/E/PES modification procedures instruction
- □ E/E/PES operation and maintenance instruction
- □ E/E/PES safety plan
- □ E/E/PES safety requirements specification
- □ E/E/PES safety requirements specification:Functions
- □ E/E/PES safety requirements specification:Integrity

Selection range
- ● IEC 61508 as a whole
- ○ Actual page only

Selection combination
- ● OR combination
- ○ AND combination

Selection type
- ● Select
- ○ Deselect
- ○ Deselect all

Those prescriptions which relate to all documents are identified by "For each document".

In this version of RiskCAT there is no single selection to choose all prescriptions related to documents.

The set of documents is based on Tables A.1 to A.3 of IEC 61508, Part 1. It is listed in Appendix 14.1 "List of Documents", page 53, of this manual.

Apart from the possibility to select according to the documents list RiskCAT offers selection according to activity (life cycle phase). Of course "documents" and "life cycle phases" are related to each other. However, in IEC 61508 a phase generally results in several documents and on the other hand a document may be used for different phases. Therefore RiskCAT uses documents as well as activities.

If you are interested in a very specific selection you should just apply a single document or activity.

If your interest is to get a complete view you should run two selections after each other:

- In one "or type" selection choose the *document* of your specific interest as well as "For each document". Terminate it with "Execute".
- In the other "or type" selection choose the *activity* related to the document of your specific interest as well as "For each activity". Terminate it again with "Execute".

CAUTION: RiskCATs assign prescriptions to documents in a restricted way.

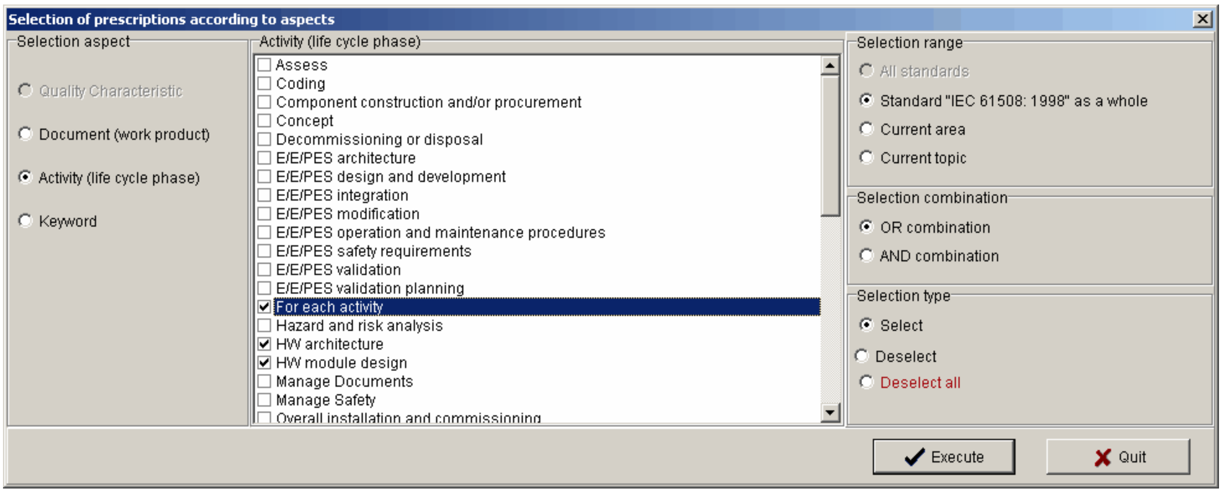
E.g. for a chapter about requirements specification it may happen that several prescriptions are not assigned to the "Requirements Specification". And if there is a series of prescriptions each related to a similar set of documents it may happen that RiskCAT assigns the first prescription to documents A and B, the second one to document C and the third one to documents D, E and F.

So, if really all prescription related to a certain document shall be identified then the selection related to the respective document needs to be added by a check of the prescriptions "near by" the already identified ones. Furthermore it needs to be taken into account that there is a certain amount of prescription valid "For each work product".

6.5 Selection of prescriptions related to activities (life cycle phases)

As with the "document" related selection functionality the "activity" related selection is activated via context menu (depress of right mouse button in the prescription window (screen part d in Figure 2)) or via the menu "Prescription selection".

After a single click on "Selection according to aspect" the selection form shown below will appear.



Selection of prescriptions according to aspects

Selection aspect
○ Quality Characteristic
○ Document (work product)
● Activity (life cycle phase)
○ Keyword

Activity (life cycle phase)
□ Assess
□ Coding
□ Component construction and/or procurement
□ Concept
□ Decommissioning or disposal
□ E/E/PES architecture
□ E/E/PES design and development
□ E/E/PES integration
□ E/E/PES modification
□ E/E/PES operation and maintenance procedures
□ E/E/PES safety requirements
□ E/E/PES validation
□ E/E/PES validation planning
☑ For each activity
□ Hazard and risk analysis
☑ HW architecture
☑ HW module design
□ Manage Documents
□ Manage Safety
□ Overall installation and commissioning

Selection range
○ All standards
● Standard "IEC 61508: 1998" as a whole
○ Current area
○ Current topic

Selection combination
● OR combination
○ AND combination

Selection type
● Select
○ Deselect
○ Deselect all

The set of activities is based on Tables A.1 to A.3 of IEC 61508, Part 1. It is listed in Appendix 14.2, "List of Activities", page 56, of this manual.

Those prescriptions which relate to all activities are identified by "For each activity".

In this version of RiskCAT there is no single selection to choose all prescriptions related to activities.

CAUTION: RiskCATs assign prescriptions to activities in a restricted way.

> E.g. for a chapter about requirements specification it may happen that several prescriptions are not assigned to "Specify requirements". And if there is a series of prescriptions each related to a similar set of activities it may happen that RiskCAT assigns the first prescription to activities A and B, the second one to activity C and the third one to activities D, E and F.
>
> So, if really all prescription related to a certain activity shall be identified then the selection related to the respective activity needs to be added by a check of the prescriptions "near by" the already identified ones. Furthermore it needs to be taken into account that there is a certain amount of prescription valid for "For each activity".

6.6 Selection of prescriptions related to key words

The "Keyword" related selection functionality is activated via context menu (depress of right mouse button) in the prescription window (screen part d in Figure 2).

The set of keywords has been created based on work with and discussion about IEC 61508 by CATS.

CAUTION: RiskCATs assign prescriptions to key words in a restricted way.

> E.g. for a series of prescriptions about CCF it may happen that RiskCAT assigns only a subset to this key word.
>
> So, if really all prescription related to a certain aspect shall be identified then the selection related to the respective key word needs to be added by a check of the prescriptions "near by" the already identified ones.

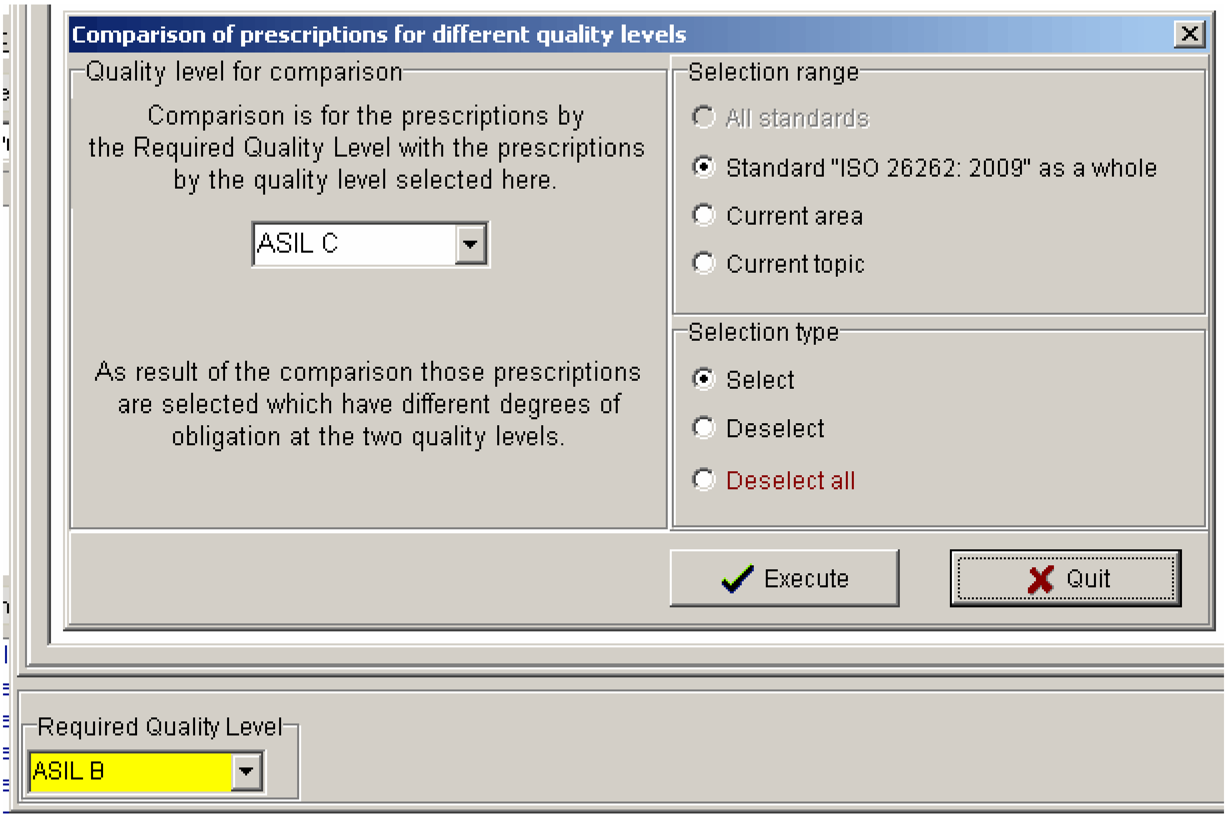
6.7 Selection of prescriptions related to quality characteristics

This is for future use.

7 Comparison of prescription's degree of obligation at different Quality Levels

Starting with version 6 RiskCAT offers the possibility to select those prescriptions which have a different level of obligation at two different SILs.

By selection of all prescriptions followed by a deselect for the different ones this results in the prescriptions which have the same degree of obligation for the given SILs.


Comparison of prescriptions for different quality levels

Quality level for comparison

Comparison is for the prescriptions by the Required Quality Level with the prescriptions by the quality level selected here.

ASIL C

As result of the comparison those prescriptions are selected which have different degrees of obligation at the two quality levels.

Selection range

○ All standards

● Standard "ISO 26262: 2009" as a whole

○ Current area

○ Current topic

Selection type

● Select

○ Deselect

○ Deselect all

Required Quality Level: ASIL B

8 Comparison of IEC 61508 with IEC 61508

This is applicable for several other RiskCATs but not for RiskCAT 61508.

9 Output of prescriptions

As basis for the production of further documents, as e. g. checklists, RiskCAT offers the possibility to export certain information as Rich Text Format (RTF) file.

For this purpose this RiskCAT version offers two presentations:

- A simple presentation which may be well edited and such easy be adopted to the formatting of existing documents.
- A formatted presentation which is used often as checklist without further editing.

Furthermore RiskCAT offers interfaces for the export of IEC 61508 prescriptions to the requirements management or to development environments. (These interfaces are available at extra expense.)

9.1 Logging the history

Starting with version 6, RiskCAT is logging its operation for purpose of reproducibility. When storing the results e. g. in File "xyz.rtf" RiskCAT stores in the same directory as "xyz.rtf" the history file named "xyz.rtf.RiskCAT_HistFile.txt".
If reproducibility may be of interest CATS suggests to save the history files together with the results themselves.

A reset on the history file is at

- RiskCAT's start
- Load Project (chapter 10.6)
- Deselect All (chapter 11.5)

Output of the history file is at

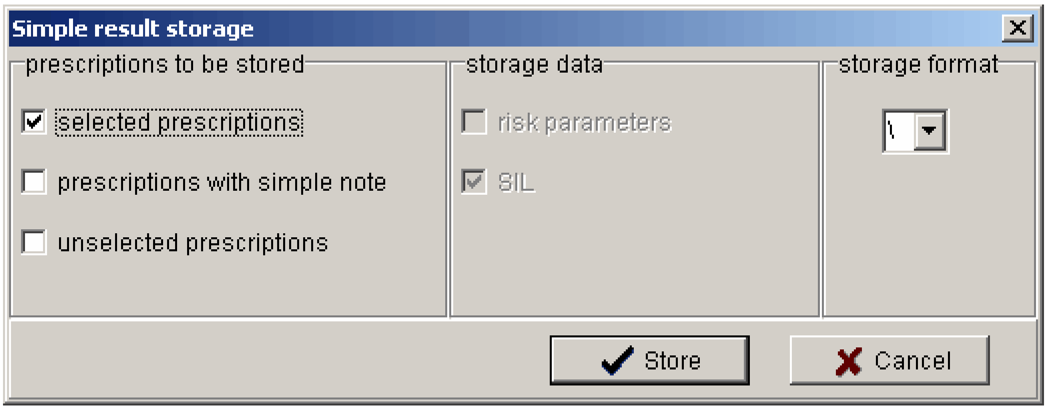
- Store Project (chapter 10.5)
- Result storage simple (chapter 9.2) and Result storage formatted (chapter 9.3)
- Export to further tools (chapters 9.4 to 9.7)

9.2 Result storage as simple text

For further documentation, e.g. creation of checklists or test plans, RiskCAT offers storage of various information separated by a Delimiter Character as text file (Rich Text Format, RTF).

This result storage is started via the menu "File" followed by a single click on "Result storage simple". For the storage there are some options given in the menu below in a self-explaining manner.

The option to select a delimiter character in the "storage format" area supports an import of the stored data in tables by a text processor. It is suggested to avoid point, colon, comma, and semicolon as delimiter because these characters are used in the prescription texts. Point, colon, and comma are used as well in the clause references.


Simple result storage

prescriptions to be stored

☑ selected prescriptions

☐ prescriptions with simple note

☐ unselected prescriptions

storage data

☐ risk parameters

☑ SIL

storage format

\

CAUTION: Purpose of the results / checklists is to use them with access to RiskCAT because RiskCAT may present the context of the checklist selection as well as the possibility for retrieval in the original standard.
Usage of the checklists without access to RiskCAT is not intended.

An example for a result storage (mandatory prescriptions for SW modification) is shown below.

Prescriptions of IEC 61508 for SIL 1 on 2008-12-08, 18:18, elaborated with RiskCAT_61508 V5.9a; English

The selected prescriptions are:

Availability of SW modification procedures prior to modification\IEC 61508, Part3: 7.8.2.1\M\

Initiation of modification by authorised request only\IEC 61508, Part3: 7.8.2.2\M\

Documented impact analysis for proposed SW modification\IEC 61508, Part3: 7.8.2.3, 7.8.2.4\M\

Modifications pertaining to earlier lifecycle phases cause return to these phases\IEC 61508, Part3: 7.8.2.5\M\

Planning including staff, specification of modification, verification, ...\IEC 61508, Part3: 7.8.2.6\M\

Modification in accordance with the plan\IEC 61508, Part3: 7.8.2.7\M\

Detailed documentation including request, configurations, ...\IEC 61508, Part3: 7.8.2.8\M\

Reverification and revalidation of data and results\IEC 61508, Part3: 7.8.2.9\M\

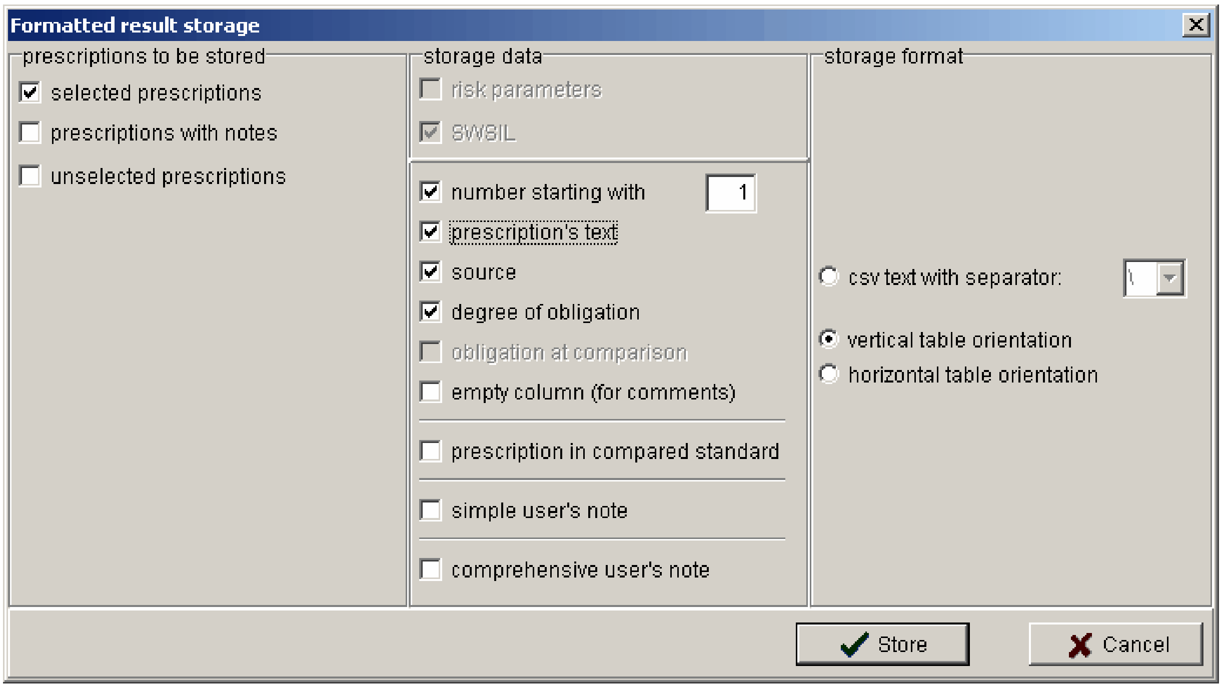
Assessment of modification depending on impact analysis and SW SIL\IEC 61508, Part3: 7.8.2.10\M\

Selection of techniques / measures to comply to these requirements:\IEC 61508, Part3: 7.8 / Table A.8\M\

9.3 Result storage as formatted text

Besides the possibility of simple format storage, which means for own formatting, RiskCAT offers storage as ready formatted Rich Text Format (RTF) table. This result storage is started via the menu "File" followed by a single click on "Result storage formatted". For the storage there are some options given in the menu below in a self-explaining manner. (For the comprehensive user's note see "10.2 Comprehensive note to the marked prescription".)

CAUTION: Purpose of the results / checklists is to use them with access to RiskCAT because RiskCAT may present the context of the checklist selection as well as the possibility for retrieval in the original standard.
Usage of the checklists without access to RiskCAT is not intended.



Formatted result storage

prescriptions to be stored
☑ selected prescriptions
☐ prescriptions with notes
☐ unselected prescriptions

storage data
☐ risk parameters
☑ SWSIL
☑ number starting with 1
☑ prescription's text
☑ source
☑ degree of obligation
☐ obligation at comparison
☐ empty column (for comments)
☐ prescription in compared standard
☐ simple user's note
☐ comprehensive user's note

storage format
○ csv text with separator: \
● vertical table orientation
○ horizontal table orientation

An example for the formatted text result storage (mandatory prescriptions for SW modification) is shown below.

Prescriptions of IEC 61508 for SIL 1 on 2008-12-08, 18:36, elaborated with RiskCAT_61508 V5.9a; English

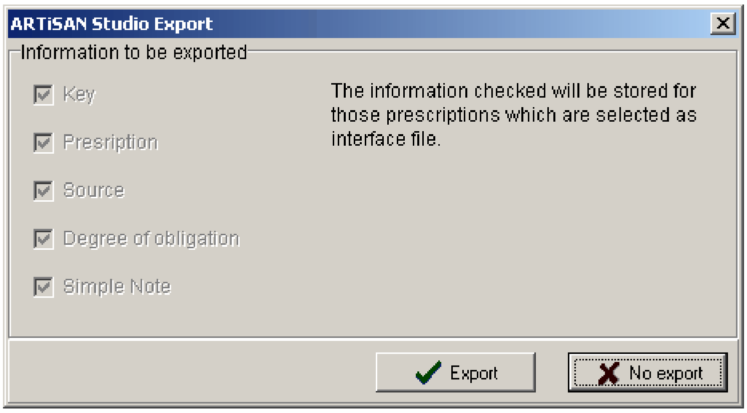
The selected prescriptions are:

1b: Control System in relation to the EUC - Modification and retrofit			
1	Planning of modification or retrofit activities prior to carrying out	IEC 61508, Part1: 7.16.2.1	M
2	Initiation of modification and retrofit by authorised request only	IEC 61508, Part1: 7.16.2.2	M
3	Request determines affected hazard, proposed change, reason	IEC 61508, Part1: 7.16.2.2	M
4	Impact analysis including assessment of the impact	IEC 61508, Part1: 7.16.2.3	M
5	Documentation of impact analysis	IEC 61508, Part1: 7.16.2.4	M

6	Authorization of modification or retrofit depending on impact analysis	IEC 61508, Part1: 7.16.2.5	M
7	Modifications impacting safety cause repetition of earlier phases	IEC 61508, Part1: 7.16.2.6	M
8	NO usage of test procedures for initial installation and commissioning for operations without checking	IEC 61508, Part1: 7.16.2.6/Note 2	M
9	Chronological documentation of modifications, analysis, reverification, ...	IEC 61508, Part1: 7.16.2.7	M
2a: Control System - Modification			
10	Maintained documentation including detailed spec of change, ...	IEC 61508, Part2: 7.8.2.1	M
11	Maintenance of a system initiating changes and informing users	IEC 61508, Part2: 7.8.2.2	M
12	Level of expertise, tools, ... for modifications at least that of initial development	IEC 61508, Part2: 7.8.2.3	M
13	Reverification and revalidation after modification	IEC 61508, Part2: 7.8.2.4	M
3b: Software, Lifecycle, but not D+D - Modification			
14	Availability of SW modification procedures prior to modification	IEC 61508, Part3: 7.8.2.1	M
15	Initiation of modification by authorised request only	IEC 61508, Part3: 7.8.2.2	M
16	Documented impact analysis for proposed SW modification	IEC 61508, Part3: 7.8.2.3, 7.8.2.4	M
17	Modifications pertaining to earlier lifecycle phases cause return to these phases	IEC 61508, Part3: 7.8.2.5	M
18	Planning including staff, specification of modification, verification, ...	IEC 61508, Part3: 7.8.2.6	M
19	Modification in accordance with the plan	IEC 61508, Part3: 7.8.2.7	M
20	Detailed documentation including request, configurations, ...	IEC 61508, Part3: 7.8.2.8	M
21	Reverification and revalidation of data and results	IEC 61508, Part3: 7.8.2.9	M
22	Assessment of modification depending on impact analysis and SW SIL	IEC 61508, Part3: 7.8.2.10	M
23	Selection of techniques / measures to comply to these requirements:	IEC 61508, Part3: 7.8 / Table A.8	M

9.4 ARTiSAN Studio export

With RiskCAT an export interface is available to ARTiSAN Studio™ by ARTiSAN Software Tools Ltd. This export interface is a package of its own and needs an extra licence.



ARTiSAN Studio Export

Information to be exported

☑ Key

☑ Presription

☑ Source

☑ Degree of obligation

☑ Simple Note

The information checked will be stored for those prescriptions which are selected as interface file.

The export is by the steps:

- Selection of the prescriptions to be exported (✓ left besides the prescription's text) and
- a single click on "ARTiSAN Studio export" in the menu "File".

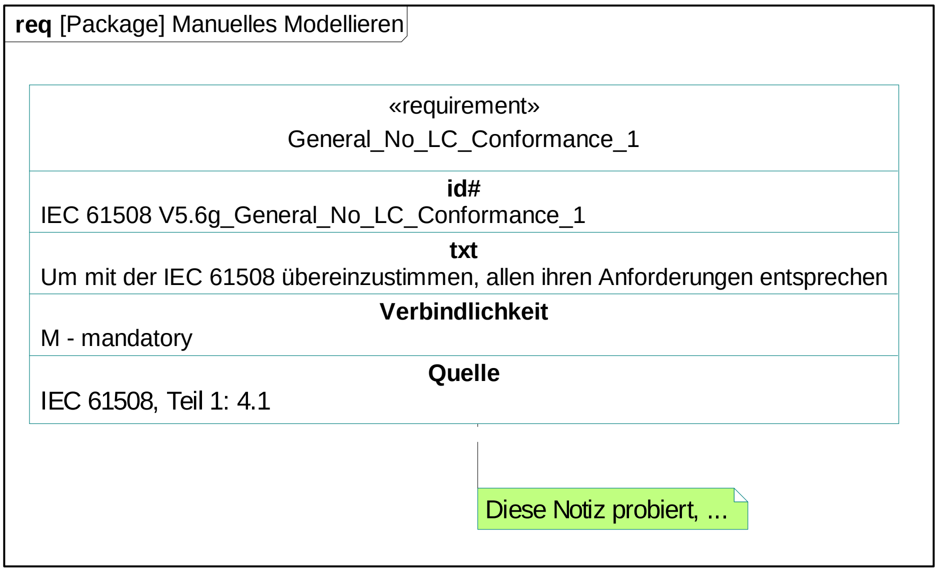
By this the form shown on the left will appear.

Export for each selected prescription is (delimiter between the values is „\£"):

- three different keys
  - „Name" of the prescription which enables ARTiSAN Studio™ to identify the prescription in a unique way. „Name" consists of (see Figure 2)
    - the area tab the prescription is assigned to,
    - the topic tab the prescription is assigned to, and
    - the line number of the prescription in its prescription window
  - „Package" of the prescription which enables ARTiSAN Studio™ to connect prescriptions which address similar contents. „Package" consists of (see Figure 2)
    - the area tab the prescription is assigned to
  - „Identifier" of the prescription which enables the traceability of the prescription back to RiskCAT. „Identifier" consists of (see Figure 2)
    - the RiskCAT database identifier (see chapter „10.7 "Help" menu"),
    - the area tab the prescription is assigned to,
    - the topic tab the prescription is assigned to, and
    - the line number of the prescription in its prescription window
- the short form of the prescription,
- the reference for the prescription in IEC 61508,
- the degree of obligation of the prescription, and
- the „Simple note" to the prescription (see chapter „10.1 Simple note to the marked prescription").

The standard used (IEC 61508), the selected SIL, date and time of the export as well as the tool identification are logged just once in the export file.

Based on the export by RiskCAT 61508 the prescriptions may imported by ARTiSAN Studio as shown in the figure below.



req [Package] Manuelles Modellieren

«requirement»
General_No_LC_Conformance_1

id#
IEC 61508 V5.6g_General_No_LC_Conformance_1

txt
Um mit der IEC 61508 übereinzustimmen, allen ihren Anforderungen entsprechen

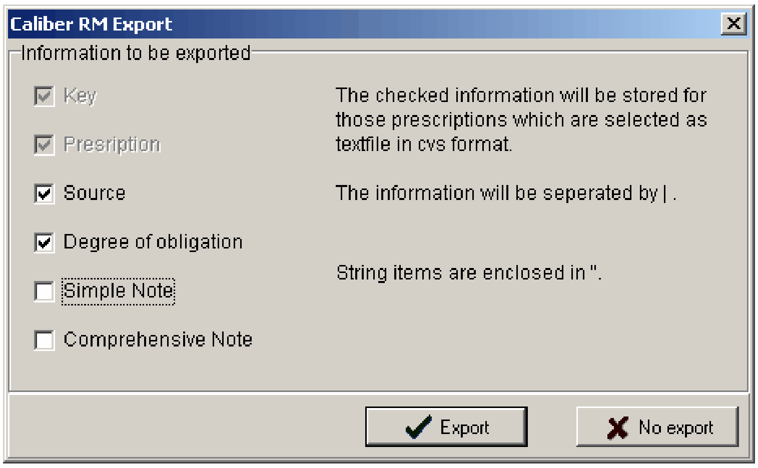
Verbindlichkeit
M - mandatory

Quelle
IEC 61508, Teil 1: 4.1

Diese Notiz probiert, ...

9.5 Caliber RM export

With RiskCAT an export interface is available to Caliber RM™ by Borland Software Corporation. This export interface is a package of its own and needs an extra licence.



Caliber RM Export

Information to be exported

☑ Key

☑ Presription

☑ Source

☑ Degree of obligation

☐ Simple Note

☐ Comprehensive Note

The checked information will be stored for those prescriptions which are selected as textfile in cvs format.

The information will be seperated by | .

String items are enclosed in ".

The export is by the steps:

- Selection of the prescriptions to be exported (✓ left besides the prescription's text) and
- a single click on "Caliber RM export" in the menu "File".

For the export itself there are some options given in the menu on the left in a self-explaining manner.

Finally the "Export" button needs to be pushed to choose the name of one of the export files and to start their generation.

Export of RiskCAT for Caliber RM are two files:

- "Export_Info.txt" with
  - the items delimiter character (|) and
  - the text enclosure character (") used for the export
- "*.cvs" with the information selected on the "Caliber export" form.

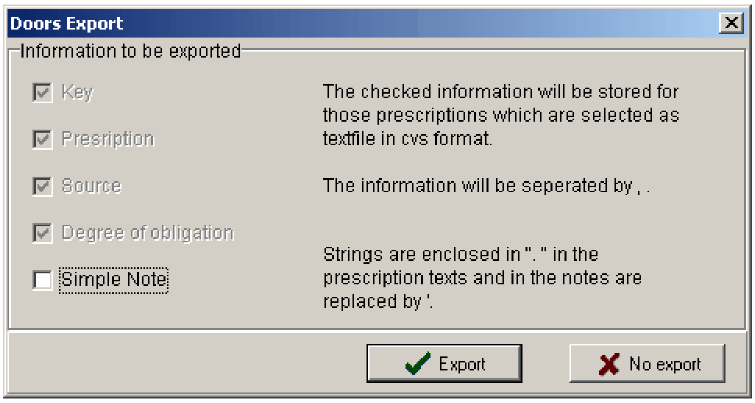
These files are inputs for the Caliber RM tools

- Import factory and
- Import utility.

The import by Caliber RM is specified in the Caliber RM user documentation. Please, apply that for the further procedure.

9.6 DOORS export

With RiskCAT an export interface is available to DOORS® by Telelogic AB. This export interface is a package of its own and needs an extra licence.



☑ Key

☑ Presription

☑ Source

☑ Degree of obligation

□ Simple Note

The checked information will be stored for those prescriptions which are selected as textfile in cvs format.

The information will be seperated by , .

Strings are enclosed in " . " in the prescription texts and in the notes are replaced by '.

The export is by the steps:

- Selection of the prescriptions to be exported (✓ left besides the prescription's text) and
- a single click on "Doors export" in the menu "File".

For the export itself there is just one option given in the menu on the left in a self-explaining manner.

Export for each selected prescription consists of (delimiter between the values is the comma; each value is enclosed in "):

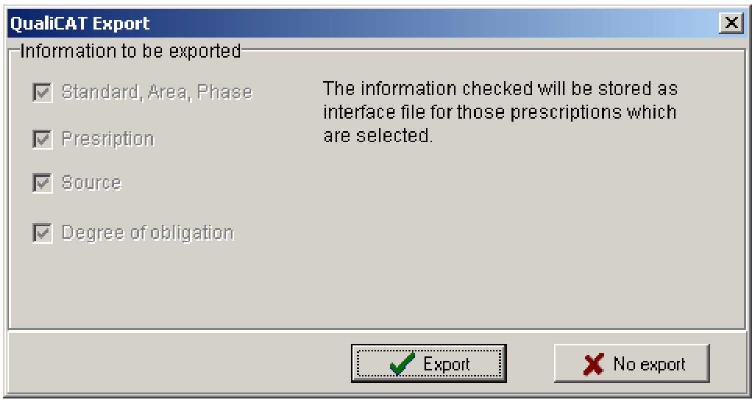
- two different keys
  - "Object Identifier" which enables DOORS® to identify the prescription in a unique way. „Object Identifier" consists of
    - an integer number assigned to the prescription.
      The "Object Identifiers" start with 2. They are consecutive when and only when all prescriptions are selected and – as a consequence – exported.
  - "RiskCAT Identifier" of the prescription which enables the traceability of the prescription back to RiskCAT. „RiskCAT Identifier" consists of (see Figure 2)
    - the RiskCAT database identifier (see chapter „10.7 "Help" menu"),
    - the area tab the prescription is assigned to,
    - the topic tab the prescription is assigned to, and
    - the line number of the prescription in its prescription window
- the short form of the prescription (" in the prescription text are replaced by '),
- the reference for the prescription in IEC 61508,
- the degree of obligation of the prescription, and
- the „Simple note" to the prescription (see chapter „10.1 Simple note to the marked prescription").

The standard used (IEC 61508), the selected SIL, date and time of the export as well as the tool identification are logged just once in the export file.

9.7 QualiCAT export

QualiCAT is the CATS tool to evaluate the compliance with a whole standard, e. g. IEC 61508, the topics of the standard or the individual prescriptions in a project or by a product during verification & validation or assessment.

The export interface to QualiCAT is part of RiskCAT.



☑ Standard, Area, Phase
☑ Presription
☑ Source
☑ Degree of obligation

The information checked will be stored as interface file for those prescriptions which are selected.

The export is by the steps:

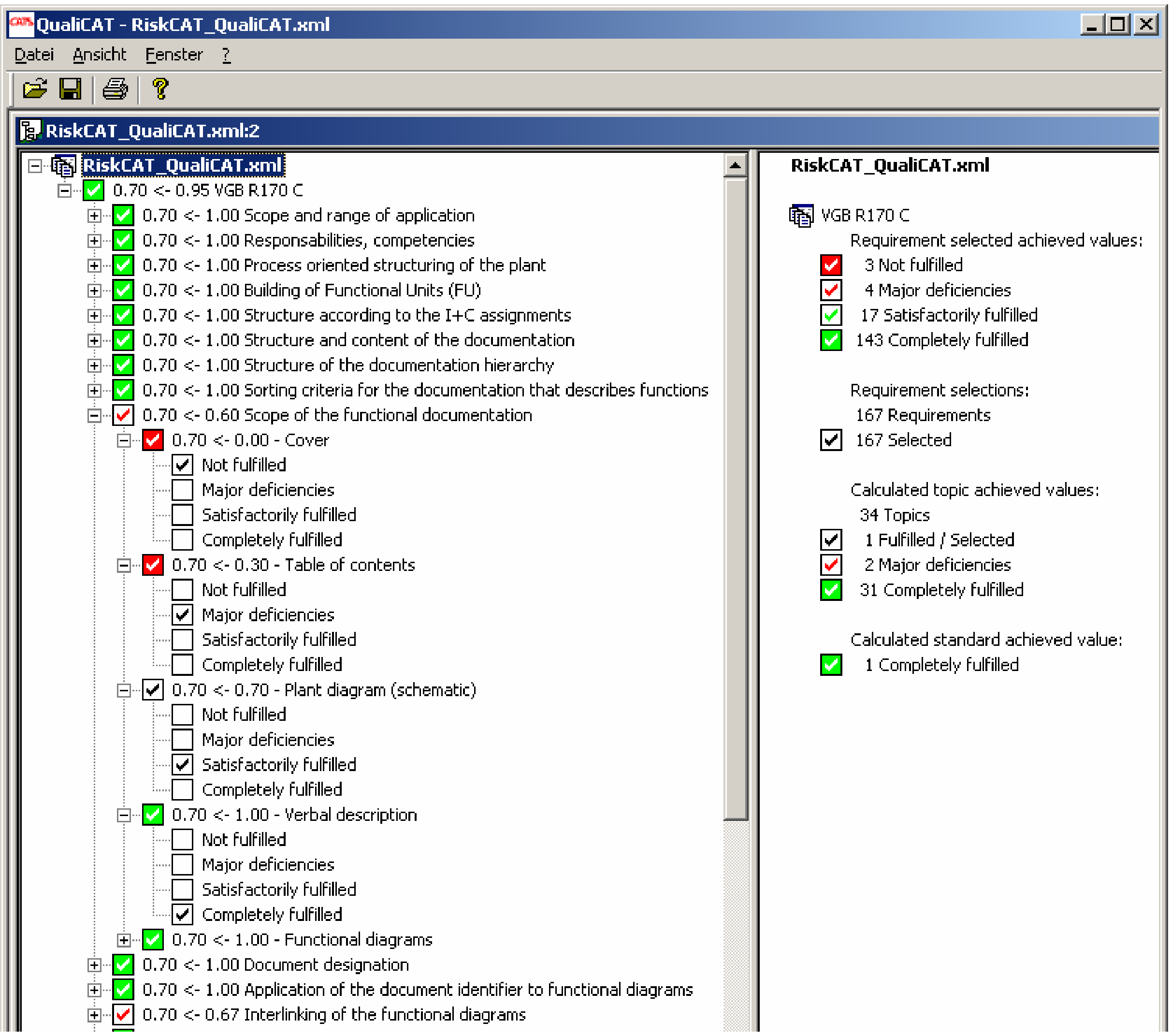
- Selection of the prescriptions to be exported (✓ left besides the prescription's text) and
- a single click on "QualiCAT export" in the menu "File".

By this the form shown on the left will appear.

Exported are in XML format as tree structure:

- the used standard (IEC 61508),
- the selected ASIL,
- the area tab the prescription is assigned to,
- the topic tab the prescription is assigned to,
- the short form of the prescription (" in the prescription text are replaced by '),
- the reference for the prescription in IEC 61508,
- the degree of obligation of the prescription,
- an initial value for the achieved compliance of the project / product under consideration with the prescription, and
- some further information .

Below an example is given for the QualiCAT output which is based on the RiskCAT export. The evaluation is about 167 prescriptions from a certain standard for power plant control systems.
The left number represents the target value for the compliance with the prescription, the topic, or the standard as a whole. These target values are computed based on the necessary SIL and the degree of obligation of the prescription.
The right numbers represent the achieved values. They are computed based on the test result, the degree of obligation, and the target values.



```
⊟ RiskCAT_QualiCAT.xml
  ⊟ ☑ 0.70 <- 0.95 VGB R170 C
     ⊞ ☑ 0.70 <- 1.00 Scope and range of application
     ⊞ ☑ 0.70 <- 1.00 Responsabilities, competencies
     ⊞ ☑ 0.70 <- 1.00 Process oriented structuring of the plant
     ⊞ ☑ 0.70 <- 1.00 Building of Functional Units (FU)
     ⊞ ☑ 0.70 <- 1.00 Structure according to the I+C assignments
     ⊞ ☑ 0.70 <- 1.00 Structure and content of the documentation
     ⊞ ☑ 0.70 <- 1.00 Structure of the documentation hierarchy
     ⊞ ☑ 0.70 <- 1.00 Sorting criteria for the documentation that describes functions
     ⊟ ☑ 0.70 <- 0.60 Scope of the functional documentation
        ⊟ ☑ 0.70 <- 0.00 - Cover
             ☑ Not fulfilled
             ☐ Major deficiencies
             ☐ Satisfactorily fulfilled
             ☐ Completely fulfilled
        ⊟ ☑ 0.70 <- 0.30 - Table of contents
             ☐ Not fulfilled
             ☑ Major deficiencies
             ☐ Satisfactorily fulfilled
             ☐ Completely fulfilled
        ⊟ ☑ 0.70 <- 0.70 - Plant diagram (schematic)
             ☐ Not fulfilled
             ☐ Major deficiencies
             ☑ Satisfactorily fulfilled
             ☐ Completely fulfilled
        ⊟ ☑ 0.70 <- 1.00 - Verbal description
             ☐ Not fulfilled
             ☐ Major deficiencies
             ☐ Satisfactorily fulfilled
             ☑ Completely fulfilled
        ⊞ ☑ 0.70 <- 1.00 - Functional diagrams
     ⊞ ☑ 0.70 <- 1.00 Document designation
     ⊞ ☑ 0.70 <- 1.00 Application of the document identifier to functional diagrams
     ⊞ ☑ 0.70 <- 0.67 Interlinking of the functional diagrams
```

```
RiskCAT_QualiCAT.xml

VGB R170 C
   Requirement selected achieved values:
☑   3 Not fulfilled
☑   4 Major deficiencies
☑  17 Satisfactorily fulfilled
☑ 143 Completely fulfilled

   Requirement selections:
  167 Requirements
☑ 167 Selected

   Calculated topic achieved values:
   34 Topics
☑   1 Fulfilled / Selected
☑   2 Major deficiencies
☑  31 Completely fulfilled

   Calculated standard achieved value:
☑   1 Completely fulfilled
```

10 Support

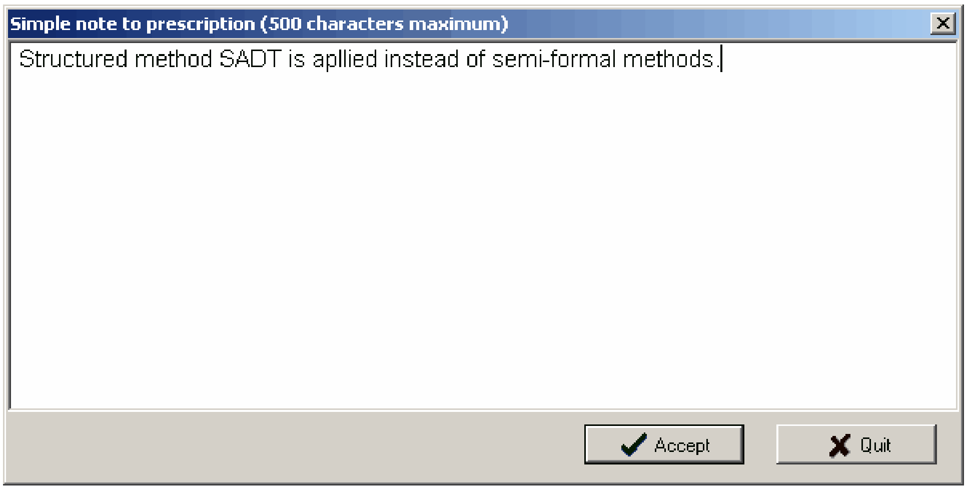
10.1 Simple note to the marked prescription

Purpose of edit notes is to provide:

- Space for comments on a specific project, e.g. to log the reasoning for not selecting particular prescriptions for the project
- Company specific frames of prescribed prescriptions as well as company specific interpretations of prescriptions
- Log results from audits, reviews, or tests.

The simple note functionality is activated via context menu in the prescription window. The steps are:

- Mark the prescription for which the note shall be edited by a single left mouse button click. Otherwise nothing visible to the user will occur.
- Activate context menu. Depress right mouse button while the pointer is in the prescription window (screen part d in Figure 2).
- Choose „Edit simple note for prescription".


Simple note to prescription (500 characters maximum)

Structured method SADT is apllied instead of semi-formal methods.

For looking to existing notes or modifying them choose "Edit simple note for prescription" again.

Prescriptions with comments are marked by ▤ left besides the prescription text. The mark is the same for a simple note, a comprehensive note (see chapter „10.2 Comprehensive note to the marked prescription"), and the usage of both notes in parallel.

Notes are saved via "Store project" (see chapter "10.5 Project (session) storage in a file" of this manual). They are reloaded by "Project load".

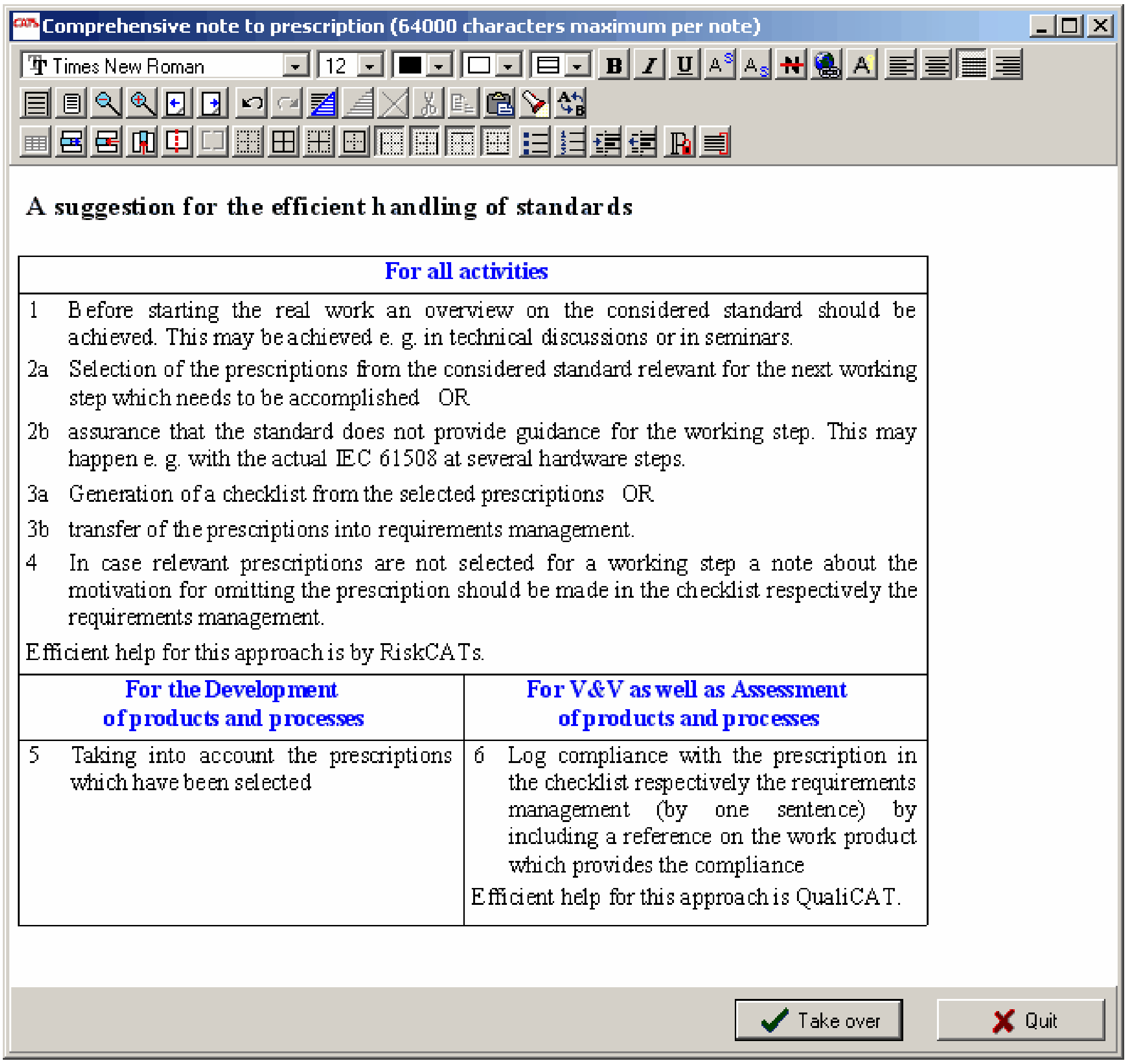
The simple notes may be exported via the prescription output (see chapter „9 Output of prescriptions"). Exception is the export to QualiCAT, because the notes may not be used by QualiCAT (until now).

CAUTION: If the results are intended to be stored as simple text file (see chapter "9.2 Result storage as simple text") usage of those characters in the note should be avoided which are intended to be the delimiter character. Otherwise the import (by the text processor applied for further processing) will be unnecessary complicated.

10.2 Comprehensive note to the marked prescription

Purpose of the comprehensive notes is the same as for the simple notes which have been the initial means of RiskCAT.

The restriction of the simple notes to 500 characters in certain cases evolved to be a significant disadvantage. So, by the comprehensive notes an extension has been the aim. The comprehensive note may be used in addition to a simple note.


Comprehensive note to prescription (64000 characters maximum per note)
Times New Roman
12
Take over
Quit

A suggestion for the efficient handling of standards

For all activities

1 Before starting the real work an overview on the considered standard should be achieved. This may be achieved e. g. in technical discussions or in seminars.

2a Selection of the prescriptions from the considered standard relevant for the next working step which needs to be accomplished OR

2b assurance that the standard does not provide guidance for the working step. This may happen e. g. with the actual IEC 61508 at several hardware steps.

3a Generation of a checklist from the selected prescriptions OR

3b transfer of the prescriptions into requirements management.

4 In case relevant prescriptions are not selected for a working step a note about the motivation for omitting the prescription should be made in the checklist respectively the requirements management.

Efficient help for this approach is by RiskCATs.

For the Development of products and processes	**For V&V as well as Assessment of products and processes**
5 Taking into account the prescriptions which have been selected	6 Log compliance with the prescription in the checklist respectively the requirements management (by one sentence) by including a reference on the work product which provides the compliance Efficient help for this approach is QualiCAT.

This sort of notes is initiated as well via the context menu. The steps are:

- Mark the prescription for which the note shall be edited by a single left mouse button click. Otherwise nothing visible to the user will occur.
- Activate context menu. Depress right mouse button while the pointer is in the prescription window (screen part d in Figure 2).
- Choose „Edit comprehensive note for prescription"

To have a look to an existing note, to modify it, or to delete it the note function is called again.

Prescriptions with comments are marked by 📄 left besides the prescription text. The mark is the same for a simple note, a comprehensive note (see chapter „10.2 Comprehensive note to the marked prescription"), and the usage of both notes in parallel.

In this RiskCAT version export of the comprehensive notes is possible only via formatted text(see chapter „9.3 Result storage as formatted text").

Notes are saved via "Store project" (see chapter "10.5 Project (session) storage in a file" of this manual). They are reloaded by "Project load".

CAUTION: In this RiskCAT version graphics and tables in notes may not be properly stored and / or exported.

CAUTION: The comprehensive notes may be exported only as part of formatted text (see chapter „9.3 Result storage as formatted text") and via Caliber RM.

10.3 Copying the actually marked prescription into the clipboard

The copy to clipboard functionality is activated via context menu in the prescription window (screen part d in Figure 2).

The steps are:

- Mark the prescription to be copied by a single left mouse button click. (Otherwise no prescription will be found on the clipboard later on.)
- Activate context menu (depress right mouse button while the pointer is in the prescription window)
- Choose "Copy selected prescription to clipboard" to copy contents of the state line
- Use an application with clipboard functionality
- Insert or paste clipboard contents

10.4 Copying from the standards into the clipboard

The copying of extracts from the standards is via the function "Copy text to clipboard" provided by XpdfViewer™ which is described in chapter 5.2, "Retrieval in the original standards".

Then the copying is in the window of the XpdfViewer. The steps are:

- Marking of the standard's region to be copied by moving the mouse with the right button pressed and then
- single left mouse button click on the symbol "copy text to clipboard" at the outmost right on the symbol bar.

After this

- start of an application with clipboard functionality and
- insertion of the clipboard contents.

10.5 Project (session) storage in a file

Project storage has two distinct purposes one for the 'normal' user and another for the project leader or the quality manager.

- For the *normal user* it offers the possibility to interrupt and resume RiskCAT tool sessions. For this purpose the actual status is stored in binary RiskCAT project files.
- For the *project leader* or the *quality manager* it offers the possibility to fill in the comments to the prescriptions. Thereby advice may be given to the 'normal' user by which means (e.g. tools, procedures, forms) compliance with the prescription shall be achieved in a specific project. If certain prescriptions are not applicable in a specific project or for a specific part of a project background for this may be supplied as comment as well. So the comments result in a company or project specific framework. This framework – or requirements capture – may be stored and used as a starting point by the 'normal' users.

The storage function is chosen by item "Store project (XML)" in the "File" menu.

Starting with version 6, RiskCAT is logging its operation for purpose of reproducibility. When storing the project e. g. in File "abc.Project.xml" RiskCAT stores in the same directory as "abc.Project.xml" the history file named "abc.Project.xml.RiskCAT_HistFile.txt".
If reproducibility may be of interest CATS suggests to save the history files together with the projects themselves.

10.6 Project (session) reload from a file

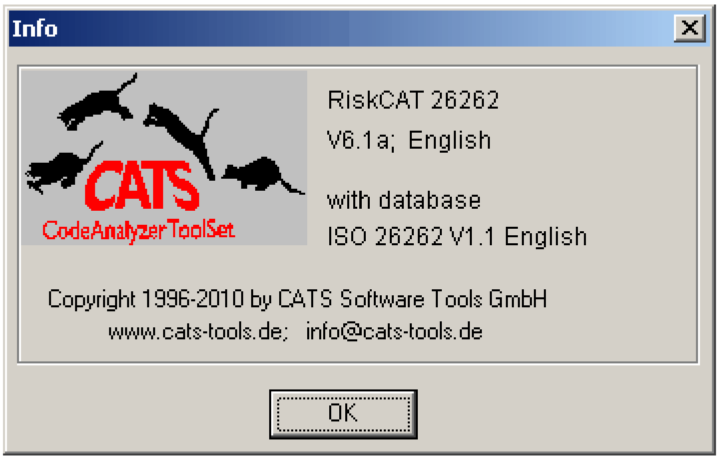
- For a new session the framework prepared by the project leader or the quality manager may be loaded.
- An interrupted and stored tool session may be resumed.

The restore function is chosen by item "Load project (XML)" in the "File" menu.

10.7 “Help“ menu

Functions within help menu are:

- Help – Main texts of this user’s manual are supplied as help.
- About – Informs about RiskCAT version and copyright



RiskCAT 26262
V6.1a; English

with database
ISO 26262 V1.1 English

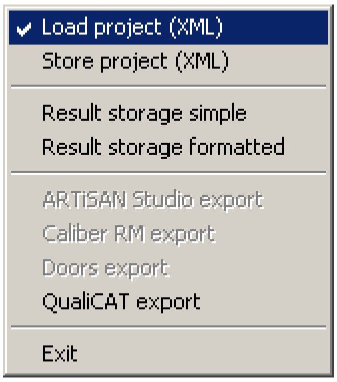
Copyright 1996-2010 by CATS Software Tools GmbH
www.cats-tools.de; info@cats-tools.de

The upper line in the besides figure identifies the tool and its version.

The lower line identifies the version of the database which is included in RiskCAT.

11 Menu functions

11.1 "File" menu



Functions within file menu are:

- Load project – see chapter "10.6 Project (session) reload from a file"
- Store project – see chapter "10.5 Project (session) storage in a file"
- Result storage simple – see chapter "9.2 Result storage as simple text"
- Result storage formatted – see chapter "9.3 Result storage as formatted text"
- ARTiSAN Studio export – see chapter "9.4 ARTiSAN Studio export"
- Caliber RM export – see chapter "9.5 Caliber RM export"
- Doors export – see chapter "9.6 DOORS export"
- QualiCAT export – see chapter "9.7 QualiCAT export"
- Exit – closes RiskCAT.

11.2 "Standard texts" menu

Functions within standards text menu are:

- Standard view by XpdfViewer™ – see chapter 5.2, "Retrieval in the original standards"

11.3 "Terms" menu

See chapter "5.5 The context related presentation of terms used in the prescription texts given in IEC 61508"

11.4 "Prescription selection" menu

See chapter "6.3 Selection of groups of prescriptions according to the degree of obligation" as well as the following ones.

11.5 "Deselect all" menu

CAUTION: Clicking this menu item causes – without additional confirmation – the deselection of all prescriptions and a reset on the history file.

11.6 “Compare SILs” menu

See chapter “7 Comparison of prescription’s degree of obligation at different Quality Levels”

11.7 “Compare Standards“ menu

Not available for RiskCAT 61508.

11.8 “Help“ menu

Functions within help menu are – see chapter “10.7 “Help“ menu”:

- Help – Main texts of this user’s manual are supplied as help.
- About – Informs about RiskCAT version and copyright

12 Context related help and hints

Already the RiskCAT versions before have been equipped with several hints.

Starting with version 5.9 some context related help has been added to RiskCAT, e. g. for the items in the menu functions. The context related help is activated via the key F1.

13 IEC 61508 specific features

Importance of IEC 61508 results from two objectives given in the scope of the standard:

- it is the basis for development of application sector international standards
- it is usable for applications without sector standards

To provide a good overall view on the prescriptions required by IEC 61508 the main part requirements and the contents of tables have been integrated as far as reasonably possible. The number of tabs has been kept acceptable low by this.

13.1 About the license for the standards supplied with RiskCAT

By contract with the German Chapter of the IEC (DKE) CATS has been asked to declare with RiskCAT[4]:

> "The data from the international standards series IEC 61508 are in use with permission of the IEC International Electrotechnical Commission, Geneva. They have not been checked by IEC or their deputies.
>
> Authoritative for the application of the standard are the versions with newest edition which may be received from VDE VERLAG GMBH, Bismarckstr. 33, D-10625 Berlin (www.vde-verlag.de). The user shall pay attention to the national standards.
>
> CATS declares that texts used correspond to the actual state of the IEC-standards.
>
> 2001-09-24, CATS"

13.2 Presentation of the degree of obligation of the requirements

Up to date IEC standards as IEC 61508 use four key words to identify their requirements (the first three explanations are from the introduction to IEC 61226):

shall	indicates requirements that are mandatory for compliance with the standard
should	indicates requirements that are not mandatory for compliance with the standard but are strongly recommended
may	indicates that compliance with the recommendation is optional
must not	indicates requirements that are mandatory for compliance with the standard ("must not" is the inverted "shall")

Furthermore IEC 61508 indicates in tables specific requirements related to Safety Integrity Levels (SIL) as highly recommended, recommended, possible, or not recommended.

[4] The original clause is in German language. Because no official translation has been available this translation is by CATS.

Within RiskCAT only one set of key words for the degree of obligation of requirements is used. To realize this

- shall requirements are classified as ‘mandatory’
- should requirements are classified as ‘highly recommended’
- may recommendations are classified as ‘possible’
- must not requirements are classified as ‘mandatory’

for all SILs.

Contents from notes and informative annexes have not been adopted to RiskCAT generally. However, in a very few cases it was felt that they are essential for application of the standard. As a consequence those are expressed explicitly in the tool.

Requirements from IEC 61508 related to production of further standards have not been implemented in RiskCAT.

13.3 About some Key-Words in the individual prescription presentation in RiskCAT

To a certain extent IEC 61508 clauses themselves give a condition for their applicability. To ease identification of these conditionally applicable clauses RiskCAT presents the respective individual prescriptions starting with the Key-Word “***IF***”. The end of the condition is denoted by “***:***”.

Some clauses “do not apply in the case of” a certain condition (e.g. clause 7.4.5 of part 2). This is presented by RiskCAT by the Key-Word “***IF NOT***”. Again the end of the condition is denoted by “***:***”.

To a certain extent again within a single IEC 61508 clause there is a choice between different prescriptions. To present this situation without splitting up the clause into too many individual prescriptions RiskCAT uses the Key-Word “***OR***” in its presentation.

To a certain extent again within a single IEC 61508 clause several prescriptions are required, e.g. several documents. To present this situation without splitting up the clause into too many individual prescriptions RiskCAT may give some of the prescriptions (the most important ones, hopefully) ending up with “***…***”.

As explained in chapter “13.2 Presentation of the degree of obligation of the requirements” there are mandatory prescriptions (key word: shall) as well as forbidden ones (key word: must not). Obligation of both is mandatory to the same extent. To arrive at a simplification we succeeded in several standards to transfer the forbidden prescriptions by inversion into mandatory ones. However, for IEC 61508 this has been successful only to a minor extent. Key words for the inversion is “***NO***”.

13.4 About the Safety Integrity Level (SIL)

The IEC 61508 provides several approaches to determine the Safety Integrity Level to be required for an E/E/PES.

CAUTION: Using these approaches you should be aware that they are informative only. So it is not appropriate to base decisions about sufficiency of a certain SIL on these approaches merely.

13.4.1 Safety Integrity Level in the quantitative approach via risk reduction

RiskCAT presents SIL 0 if a rate of dangerous failures $\geq 10^{-1}$/demand may be accepted.

RiskCAT presents SIL 4 if the rate of dangerous failures needs to be $<10^{-5}$/demand. Additionally RiskCAT then presents (only) in the window for the approach "Risk reduction": "Necessary SIL is > 4; …".

13.4.2 Safety Integrity Level in the Risk Graph Approach

Below SIL 1 the IEC 61508 (part 5, figures D.1 and D.2) denotes the SILs as "No safety requirements" and "No special safety requirements". Instead of this wording RiskCAT uses SIL 0. However, the wording of the standard is presented in addition to the SIL number.

Beyond SIL 4 the IEC 61508 (part 5, figures D.1 and D.2) denotes the SIL as "A single E/E/PES is not sufficient" or "An E/E/PE SRS is not sufficient". In addition to this wording RiskCAT chooses SIL 4.

13.4.3 Safety Integrity Level in the Probabilistic Approach

Table 3 of IEC 61508, part 1, is the basis for the probabilistic approach with RiskCAT. It is restricted to a variation of the probability of a dangerous failure to 4 orders of magnitude from $\geq 10^{-9}$/hour to $<10^{-5}$/hour. In case the rate of dangerous failures may be $\geq 10^{-5}$/hour or needs to be $<10^{-9}$/hour IEC 61508 does not provide any SIL.

RiskCAT results in SIL 0 if the rate of dangerous failures may be $\geq 10^{-5}$/hour.

RiskCAT results in SIL 4 if the rate of dangerous failures needs to be $<10^{-9}$/hour and denotes the SIL as "SIL not valid".

13.4.4 Safety Integrity Level 0

RiskCAT developers feel that there is no clear prescription within IEC 61508 about the degree of obligation of the required prescriptions below SIL 1. So RiskCAT for SIL 0 assigns the lowest degree of obligation which is 'possible' to all prescriptions. In case user feels this approach to be too weak it is suggested to increase the SIL manually from 0 to 1.

13.5 About part 1 of the standard

Requirements within **Part 1** - General Requirements - are independent of SIL except three requirement. They are presented in RiskCAT tab 'Assessment'. Part 1 does not make use of alternative requirements offering the possibility to choose between different approaches.

Within Part 1 there are requirements requiring that part 2 or 3 or certain clauses of those parts shall be applied. This type of requirement has been skipped for purpose of RiskCAT.

Actual database for part 1 is based on pdf file dated 10.08.1999, size 643 897 Bytes containing the 'First edition' of the standard dated '1998-12'. That pdf includes the contents of the corrigendum 1 of April 1999.

Most Part 1 requirements are from clause 7, Overall safety lifecycle requirements. RiskCAT presents these requirements in its area

- "1b: Control System in relation to the EUC"

All other Part 1 requirements are presented in RiskCAT area

- "1a: General".

13.6 About part 2 of the standard

Part 2 - which is about system requirements - makes use of SIL dependent requirements in 8 tables of its annexes which are about selection of techniques and prescriptions. Alternative requirements offering the possibility to choose between different techniques and prescriptions are used in these tables to some extent as well. RiskCAT presents those alternative sets of prescriptions by grey shaded background.

Within Part 2 there are requirements requiring that part 1 or certain clauses of this part shall be applied. This type of requirement has been skipped for purpose of RiskCAT.

Tables A.16 to A.18 as well as B.1 to B.5 besides the importance require a certain SIL dependent effectiveness. Effectiveness requirements are special for part 2. They are not presented in actual RiskCAT version.

The prescriptions grouping in tables B.1 and B.4 as well as second grouping in table B.5 with the opportunity to choose just one method are valid only for 'R' prescriptions. Choice is not allowed for 'HR' prescriptions. Again this importance related grouping is special for part 2. It is not presented in actual RiskCAT version.

Actual database for part 2 is based on file dated 06.11.2000, size 919 951 Bytes containing the 'First edition' of the standard dated '2000-05'. All requirements contained in part 2 are given in clause 7, Lifecycle requirements on the E/E/PES.

On the one hand side these requirements are concerned with the control system as a whole (hardware plus software). These requirements are presented in RiskCAT area

- "2a. Control System".

On the other hand side these requirements are concerned just with the hardware only. These requirements are presented in RiskCAT area

- 2b. Hardware

Capturing the required prescriptions from IEC 61508, CATS felt that in part 2 there are three areas of weaknesses:

- It has been understood that IEC 61508 uses *"failure"* for the effect that E/E/PES does supply its specified function. And it has been understood that IEC 61508 uses *"random failure"* for the physical transition of a hardware device to defect. However, in several cases feeling was that *"failure"* has been used instead of *"random failure"*. For the RiskCAT prescriptions a clear distinction between *"failure"* and *"random failure"* has been tried.
- Most clauses of IEC 61508, part 2, are valid for the E/E/PES as a whole. Others are valid just for the hardware part. For the RiskCAT prescriptions a clear distinction between those two areas of validity has been tried by assigning them to the two areas "2a. Control System" and "2b. Hardware".
- With respect to integration tests
  - Part 1, Table A.2, mentions "Specification (integration tests of programmable electronic and non programmable electronic hardware)". In part 2, 7.5.2, neither the document is mentioned nor a related activity.
  - Part1, Table A.2 mentions "Specification (hardware architecture integration tests)". In part 2, 7.5.2, neither the document is mentioned nor a related activity.
  - Part 2, 7.4.2.11, suggests that an „E/E/PES integration tests specification" should exist which is suggested by 7.5.2.1 as well. However, this spec is not contained in Part1, Table A.2
  - as a conclusion RiskCAT uses
    * E/E/PES integration tests specification.
    However, it does not use
    * Specification (integration tests of programmable electronic and non programmable electronic hardware)"

13.7 About part 3 of the standard

As part 2 the **part 3** - which is about software requirements - makes extensive use of SIL dependent requirements in its annexes which are about selection of techniques and prescriptions. Alternative requirements offering the possibility to choose between different techniques and prescriptions are used in annexes to some extent as well. RiskCAT presents those alternative sets of prescriptions by grey shaded background.

Actual database for part 3 is based on pdf file dated 10.08.1999, size 537 549 Bytes containing the 'First edition' of the standard dated '1998-12'. That pdf includes the contents of the corrigendum 1 of April 1999.

Most Part 3 requirements are from clause 7, Software safety lifecycle requirements. RiskCAT presents these requirements in its areas

- "3c. Software, Design and development (D+D)" and
- "3b. Software, Lifecycle, but not D+D".

All other Part 3 requirements are presented in RiskCAT area

- “3a. Software, Non Lifecycle”.

The Tables of Part 3, Appendix A, are not refining a special requirement but provide techniques and prescriptions for a whole chapter of the standard. So to ease overview and keep low the number of topic tabs the contents of the tables from Appendix A are presented together with the main part requirements as far as they are concerned with just one chapter. However, to provide the possibility of easy identification of the techniques / prescriptions from the appendix they are preceded by a “- “.

To increase clarity RiskCAT 61508 is listing the three prescriptions by Table B.6, „Performance testing“, twice. They are listed as well in area “3b. Software, Lifecycle, but not D+D” as in area “3c. Software, Design and development (D+D)”.

13.8 About the other parts of the standard

Part 5 - which is about the determination of safety integrity levels - does not involve any requirement. However extensive use has been made of this part in realizing the group box ‘IEC 61508 risk’. Therefore RiskCAT offers the opportunity to access the part if related PDF file is available.

Part 4 is about terms only. It is used by RiskCAT for purpose of the context related presentation of terms (see 5.5, “The context related presentation of terms used in the prescription texts given in IEC 61508”; Normal Package only).

Part 6 and **part 7** are examples and explanations. They are used by RiskCAT for purpose of the context related presentation of explanations, especially part 7 (see 5.4, “The context related presentation of explanations to the clause provided by IEC 61508 itself”; Normal Package only). Again RiskCAT offers the opportunity to access the part if related PDF file is available.

13.9 Abbreviations used in the RiskCAT Database

ALARP	As low as reasonably practicable
DB	Database
D+D	Design and development
E/E/PES	Electrical / electronic / programmable electronic system
EUC	Equipment under control
HW	Hardware
IF	see chapter “13.3 About some Key-Words in the individual prescription presentation in RiskCAT”
NO	see chapter “13.3 About some Key-Words in the individual prescription presentation in RiskCAT”
OR	see chapter “13.3 About some Key-Words in the individual prescription presentation in RiskCAT”
SFC	Systematic faults control
SIL	Safety integrity level
SW	Software
V+V	Verification and validation
…	see chapter “13.3 About some Key-Words in the individual prescription presentation in RiskCAT”

14 Appendix

14.1 List of Documents

RiskCAT takes the documents listed as examples in IEC 61508, Part 1, tables A.1, A.2 and A.3 (pages 103, 105, 107) as presented in the following table.

The names used in these tables partly have been slightly modified, e.g. "Plan (safety)" from table A.1 to "Overall safety plan" in RiskCAT.

The documents in colour are documents in pairs:

- Yellow plans are related to green reports (and one log)
- Cyan plans and specifications are related to magenta reports

Some of the documents listed in tables A.1, A.2 and A.3 are not addressed by the IEC 61508 prescriptions (and such not by RiskCAT as well). Those are marked by ☹.

<table>
<tr><th colspan="2">Document</th><th>Table</th></tr>
<tr><td colspan="2">Overall safety plan
Overall verification plan
Overall functional safety assessment plan

Overall concept description
Overall scope description
Hazard and risk analysis description
Overall safety requirements specification, comprising
• Overall safety functions requirements specification and
• Overall safety integrity requirements specification
Safety requirements allocation description
Overall operation and maintenance plan
Overall validation plan
Overall installation plan
Overall commissioning plan</td><td>A.1</td></tr>
<tr><td colspan="2">E/E/PES safety plan
E/E/PES verification plan
E/E/PES functional safety assessment plan ☹
(for the related clauses please refer to Overall functional safety assessment plan)

E/E/PES safety requirements specification, comprising:
• E/E/PES safety functions requirements specification and
• E/E/PES safety integrity requirements specification
E/E/PES validation plan
E/E/PES architecture design description, comprising:
• HW architecture design description and
• SW architecture design description
E/E/PES integration tests specification (integration of programmable electronic and non programmable electronic hardware to E/E/PES)</td><td>A.2</td></tr>
<tr><td><em>Hardware
(from Table A.2)</em></td><td><em>Software
(from Table A.3)</em></td><td></td></tr>
<tr><td></td><td>SW safety plan
SW verification plan
SW functional safety assessment plan ☹</td><td></td></tr>
</table>

Document		Table
PE integration tests specification ☹ HW architecture design description HW architecture integration tests specification ☹ (no report to this spec in A.2) HW module design specification HW modules test specification ☹ HW modules ☹ HW modules test report ☹ PE integration test report ☹	SW safety requirements specification, comprising: • SW safety functions requirements specification and • SW safety integrity requirements specification SW validation plan PE integration tests specification SW architecture design description SW architecture integration tests specification Development tools instruction ☹ Coding manual SW system design description SW system integration tests specification SW module design specification SW module tests specification Source code list Code review report ~~SW module test report~~ [5] SW module test report SW module integration test report (no spec for this test) SW system integration test report ☹ SW architecture integration test report ☹ PE integration test report SW validation report	
	SW user instruction SW operation and maintenance instruction SW modification procedures instruction SW modification request SW modification impact analysis report SW modification log SW verification report SW functional safety assessment report ☹	
E/E/PES integration test report (programmable electronic and other hardware integration test) E/E/PES user instruction E/E/PES operation and maintenance instruction E/E/PES validation report E/E/PES modification procedures instruction E/E/PES modification request ☹ E/E/PES modification impact analysis report E/E/PES modification log E/E/PES verification report E/E/PES functional safety assessment report ☹		A.2

[5] The SW module test report is the only document mentioned twice in IEC 61508, part 1, table A.3. In IEC 61508, part 3, table 1 it is only mentioned as result of the Software module testing. However it is not mentioned as result of code implementation. So for purpose of clearness it has been deleted here as a result of code implementation.

Document	Table
(for the related clauses please refer to Overall functional safety assessment report)	
Overall installation report Overall commissioning report Overall validation report Overall operation and maintenance log Overall modification and retrofit • request • impact analysis report • log Overall decommissioning or disposal • impact analysis report • plan • log Overall verification report Overall functional safety assessment report	A.1

For RiskCAT following documents have been added to those given by IEC 61508:

- QM System
- Component
- Code:Machine
- Overall modification and retrofit procedures instruction (because of part 1, clause 6.2.1.l)
- For each document
  (By this those prescriptions are selected which relate to all documents.
  In this version of RiskCAT there is no single selection to choose all prescriptions related to documents.)

14.2 List of Activities

RiskCAT takes the activities listed as examples in IEC 61508, Part 1, tables A.1, A.2 and A.3 (pages 103, 105, 107) as presented in the following table.

<table>
<tr><th colspan="2">Activity</th><th>Table</th></tr>
<tr><td colspan="2">Concept
Overall scope definition
Hazard and risk analysis
Overall safety requirements
Safety requirements allocation
Overall operation and maintenance planning
Overall validation planning
Overall installation and commissioning planning
Realisation (see tables A.2 and A.3)</td><td>A.1</td></tr>
<tr><td colspan="2">E/E/PES safety requirements
E/E/PES validation planning
E/E/PES design and development
E/E/PES architecture</td><td>A.2</td></tr>
<tr><td>From Table A.2</td><td>From Table A.3</td><td></td></tr>
<tr><td>Hardware architecture
Hardware module design
Component construction and/or procurement</td><td>Software safety requirements
Software validation planning
Software design and development
Software architecture
Software system design
Software module design
Coding
Software module testing
Software integration</td><td></td></tr>
<tr><td>Programmable electronic integration</td><td>Programmable electronic integration
Software operation and maintenance procedures
Software safety validation
Software modification</td><td></td></tr>
<tr><td colspan="2">E/E/PES integration
E/E/PES operation and maintenance procedures
E/E/PES validation
E/E/PES modification</td><td>A.2</td></tr>
<tr><td colspan="2">Overall installation and commissioning
Overall validation
Overall operation
Overall maintenance
Overall modification and retrofit
Decommissioning or disposal</td><td>A.1</td></tr>
</table>

For RiskCAT following activities have been added to those given by IEC 61508:

- Assess
- Manage Documents
- Manage Safety
- Reliability Computation
- Review
- For each activity
  (By this those prescriptions are selected which relate to all activities.
  In this version of RiskCAT 61508 there is no single selection to choose all prescriptions related to activities.)